EXHIBIT B-4

and was partially complete by June 29, 2015.[722] As of August 18, 2015, OPM determined that as many as twenty-four devices were still "communicating with the CyFIR server."[723]

The documents show CyTech provided significant incident response and forensic support from April 23 through May 1, 2015. CyTech continued to provide services as needed after CyTech personnel were no longer on site at OPM. Further, OPM deployed the CyFIR tool beginning in April 2015 and did not fully uninstall it until August 2015.[724] The documents also show the CyFIR tool was still installed and communicating with the CyFIR server as late as August 2015. CyTech relied on OPM's request for assistance on April 22, 2015 and provided incident response and forensic support services. Then CyTech became the unwilling focus of media attention.

The *Wall Street Journal* Reports on CyTech's Role in the OPM Incident on June 10, 2015

Pieces of the CyTech story became public when the *Wall Street Journal* published a story under the headline "U.S. Spy Agencies Join Probe of Personnel-Records Theft" on June 10, 2015.[725] The story stated:

> Last week, the Office of Personnel Management disclosed that hackers had breached its networks, warning that the personnel records of roughly four million people—many of them current or former government workers—could have been stolen. At the time, OPM said the breach was discovered as the agency 'has undertaken an aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks.'
>
> But four people familiar with the investigation said the breach was actually discovered during a mid-April sales demonstration at OPM by a Virginia company called CyTech Services, which has a networks forensics platform called CyFIR. CyTech, trying to show OPM how its cybersecurity product worked, ran a diagnostics study on OPM's network and discovered malware was embedded on the network. Investigators believe the hackers had been in the network for a year or more.
>
> An OPM spokesman didn't respond to a request for comment.[726]

---

[722] Email from Administrator, U.S. Office of Pers. Mgmt., to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Aug. 19, 2015, 11:34 a.m.) at HOGR0909-000160 (OPM Production: Oct. 28, 2015).
[723] Email from Administrator, U.S. Office of Pers. Mgmt., to Brendan Saulsbury Senior Cyber Security Engineer, SRA, and Jonathan Tonday, Contractor, U.S. Office of Pers. Mgmt. (Aug. 18, 2015, 11:32 a.m.) at HOGR0909-000125 (OPM Production: Oct. 28, 2015).
[724] Cotton Tr. at 61.
[725] Damian Paletta & Siobhan Hughes, *U.S. Spy Agencies Join Probe of Personnel-Records Theft*, WALL STREET JOURNAL, June 10, 2015, available at: http://www.wsj.com/articles/u-s-spy-agencies-join-probe-of-personnel-records-theft-1433936969.

The Committee obtained communications between OPM and CyTech related to the media inquiry. The documents show that before the article was published, CyTech coordinated with OPM. There is no evidence to suggest CyTech was the source of the story. Cotton testified:

> We did not intend to find ourselves in the middle of these hearings. And I am just very concerned about the representations that may or may not have been made around this Hill that have actually been relayed to me that OPM is maligning my company's reputation and our capabilities.[727]

CyTech Coordinated with OPM Prior to the June 10, 2015 Story

On June 9, 2015, Cotton received a call from a reporter regarding CyTech's role in the discovering the OPM data breach.[728] The reporter told Cotton he had four sources saying that CyTech discovered the OPM breach and that CyTech had been advising OPM about this matter for the last year.[729] The reporter requested a comment.[730] Cotton said the reporter could email him about the story, but that he would not comment.[731] Cotton wanted something in writing to confirm the identity of the person on the call.[732]

Late on June 9, 2015, Cotton reviewed the email from the reporter and immediately forwarded it to Wagner for guidance.[733] Cotton asked whether he wanted CyTech to make corrections.[734] Wagner said, "Correct away. Just give me a heads up as to the response so we can discuss."[735]

Cotton proposed a response to the reporter: "[I]t is CyTech policy to not discuss clients or operational matters with the press. CyTech can categorically deny that personnel from CyTech advised OPM personnel concerning this matter a year ago . . . ."[736] Wagner responded early the next day and suggested what amounted to a "no comment" response. Wagner wrote: "[if you] need anything feel free to fire back. Keep the faith."[737]

---

[726] Damian Paletta & Siobhan Hughes, *U.S. Spy Agencies Join Probe of Personnel-Records Theft*, WALL STREET JOURNAL, June 10, 2015, http://www.wsj.com/articles/u-s-spy-agencies-join-probe-of-personnel-records-theft-1433936969.
[727] Cotton Tr. at 107.
[728] Cotton Tr. at 64
[729] *Id.*
[730] *Id.*
[731] *Id.*
[732] *Id.*
[733] Cotton Tr. at 64-65.
[734] Cotton Tr., Ex. 9 (Email from Ben Cotton, Chief Exec. Officer, CyTech, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 9, 2015)).
[735] *Id.*
[736] *Id.*
[737] Email from Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt., to Ben Cotton, Chief Exec. Officer, CyTech (June 10, 2015, 7:14 a.m.) at 2.4 (CyTech Production: Aug. 19, 2015).

OPM and CyTech Respond to the Article

On June 10, 2015, the story was published. It stated: "[F]our people familiar with the investigation said the [OPM] breach was actually discovered during a mid-April sales demonstration at OPM by a Virginia company called CyTech Services, which has a network forensics platform called CyFIR."[738] Wagner testified that this portion of the story was not "accurate in any way."[739]

The story further stated: "CyTech, trying to show OPM how its cybersecurity product worked, ran a diagnostics study on OPM's network and discovered malware was embedded on the network."[740] Coulter, the Cylance engineer onsite at the time of the CyTech demonstration,[741] testified with respect to that portion of the story: "that's actually accurate. They did. They ran a diagnostic study. They may have discovered malware that was embedded on the network, but it was likely already known at that point."[742]

On June 12, 2015, Wagner emailed CyTech about the story. Wagner wrote: "I cannot express how bad this is going down for you. We should talk about this. Call my cell."[743] Cotton quickly responded: "just tried to call. THE LEAKS ARE NOT US!!!" (*emphasis in the original*).[744] In response, Wagner suggested a call with OPM's public affairs office to "work out something that will benefit both organizations."[745] Cotton agreed to discuss the situation.[746]

From: Ben Cotton [redacted]
Sent: Friday, June 12, 2015 9:07 AM
To: Wagner, Jeffrey P.
Subject: Re: CyFIR talking to press and making claims about OPM?

Jeff,

Just tried to call. THE LEAKS ARE NOT US!!!!

V/R,

Ben
Ben Cotton
President/CEO
Cytech Services

---

[738] Damian Paletta & Siobhan Hughes, *U.S. Spy Agencies Join Probe of Personnel-Records Theft*, WALL STREET JOURNAL, June 10, 2015, available at: http://www.wsj.com/articles/u-s-spy-agencies-join-probe-of-personnel-records-theft-1433936969.
[739] Wagner Tr. at 156.
[740] Damian Paletta & Siobhan Hughes, *U.S. Spy Agencies Join Probe of Personnel-Records Theft*, WALL STREET JOURNAL, June 10, 2015, http://www.wsj.com/articles/u-s-spy-agencies-join-probe-of-personnel-records-theft-1433936969.
[741] OPM Visitor Logs, Washington, D.C. (April 21, 22, 2016) at HOGR020316-000521, 524 (OPM Production: Feb. 16, 2016).
[742] Coulter Tr. at 61, Ex. 9.
[743] Cotton Tr., Ex. 10 (Email from Ben Cotton, Chief Exec. Officer, CyTech, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 12, 2015)).
[744] *Id.*
[745] *Id.*
[746] Cotton Tr. at 66, Ex. 10.

In describing OPM's phone conversations with CyTech to the Committee, Wagner testified he had two calls with Cotton on or about June 12, during which the CyTech CEO "acted shocked, assured me it was not him or his company" who had leaked the story.[747] Cotton testified he was surprised by OPM's reaction on the first call and learned OPM was concerned about the story because "the account in the *Wall Street Journal* was inconsistent as to how OPM leadership had already testified to Congress."[748]

Wagner testified that during the second call with OPM's public affairs staff, Cotton again said CyTech was not the source of the story, but he believed Cotton was telling the *Wall Street Journal* that CyTech did in fact have some role in the discovery of the breach.[749]

Cotton, on the other hand, testified that OPM wanted CyTech to sign on to a joint statement that "in essence, it was that *Wall Street Journal* was totally without basis, without fact, and was a lie."[750] Cotton also testified he requested a written draft of OPM's suggested statement, but OPM declined and ultimately CyTech did not agree to their approach because it was "not what actually occurred."[751]

Cotton testified that he explained the whole situation to OPM's public affairs staff, including the April 21, 2015 product demonstration and CyTech's role in incident response and forensic support.[752] Cotton testified that OPM's press spokesman seemed surprised and said he would be in touch, but CyTech did not hear from OPM again.[753] After multiple press inquiries following the story, CyTech issued a press release on June 15, 2015. The press release stated:

> It is CyTech's policy not to discuss our clients or their sensitive operations. However, due to extensive media reporting, we wanted to clarify CyTech's involvement and the assistance we provided in relation to OPM's breach response in April 2015. . . CyTech was initially invited to OPM to demonstrate CyFIR Enterprise on April 21, 2015. . . Using our endpoint vulnerability assessment methodology, CyFIR quickly identified a set of unknown processes running on a limited set of endpoints. This information was immediately provided to the OPM security staff and was ultimately revealed to be malware. CyTech is unaware if the OPM security staff had previously identified these processes. CyTech Services remained on site to assist with the breach response, provided immediate assistance, and performed incident response supporting OPM until May 1, 2015.[754]

---

[747] Wagner Tr. at 153.
[748] Cotton Tr. at 66.
[749] Wagner Tr. at 154.
[750] Cotton Tr. at 68.
[751] *Id.*
[752] *Id.*
[753] Cotton Tr. at 68-69.
[754] Cotton Tr., Ex. 14 (CyTech, Press Release, *CyTech Services Confirms Assistance to OPM Breach Response* (June 15, 2015)). CyTech did produce a draft press release dated June 10, 2015 to the Committee that the CyTech CEO quickly identified as a draft document when questioned about it. This draft press release did not precisely describe CyTech's involvement. The CyTech CEO explained that he revised this draft to the version released June 15 since this was a "public statement against a very large and very powerful government organization, I needed to

The *Wall Street Journal* covered CyTech's public statement in a follow up article on June 15, 2015.[755] In the story, an OPM official stated: "the assertion that Cytech was somehow responsible for the discovery of the intrusion into OPM's network during a product demonstration is inaccurate."[756]

Cotton testified that when he heard OPM's statement, he was concerned because the dispute was starting "to impact our corporate reputation and our capabilities," and he speculated that OPM was parsing words by using the term "discovery of the breach."[757] Cotton testified that "the challenge we had here was clearly you don't want to get into a fight with in the news with one of your clients. But at the same time, to say we had no part in the discovery was clearly false . . . ."[758] Cotton testified that "discovery of the breach" is not precisely defined, and that in his mind, CyTech had "discovered" malware on the system.[759] Cotton stated it was possible "that had somebody noticed a packet going out to an unknown Web site that they could then say, well, we discovered that, because we saw this packet."[760]

The documents show the statement issued by CyTech on June 15, 2015 is consistent with the facts. The documents show CyTech did play a role in identifying malware in the live OPM IT environment and providing incident response and forensic support to OPM beginning in mid-April 2015. The documents show CyTech did not publicly claim to have discovered the intrusion, but rather that it played a role in identifying malware. The agency's strong reaction to the June 10, 2015 story in the *Wall Street Journal* was based on a concern that it contradicted statements senior officials made to Congress about the data breach.[761]

It is troubling that CyTech appears to have in good faith worked to coordinate with OPM on responses to the press while OPM worked to "**kill this cytech crap.**"[762] OPM press officials also demanded that the WSJ print a retraction of the CyTech story on June 10, the day the story

---

be very precise about what my company did and what we didn't do to avoid any entanglements with definitions over "breach discovery." Cotton Tr. at 84-85.

[755] Damian Paletta, *Cybersecurity Firm Says It Found Spyware on Government Network in April*, WALL ST. J., June 15, 2015, available at: http://www.wsj.com/articles/firm-tells-of-spyware-discovery-in-government-computers-1434369994.

[756] *Id.*

[757] Cotton Tr. at 70.

[758] *Id.*

[759] Cotton Tr. at 71.

[760] *Id.*

[761] Cotton Tr. at 66.

[762] Email from Sam Schumach, Press Sec., U.S. Off. of Pers. Mgmt. to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. and Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt. (June 18, 2015, 1:25 p.m.) at HOGR020316-000261 (OPM Production: Feb. 16, 2016). OPM appears to have become frustrated with the CyTech story. In a June 23, 2015 email, the OPM Dir. of Communications was coordinating a response to the WSJ on a cybersecurity issue and said to Mr. Wagner, "do you have time to get on the phone with [the reporter] for 10 minutes. I want to make sure he's not trying to resurrect the CyTech Dracula here, in a subtle way." Email from Jackie Koszczuk, Dir. of Comm., U.S. Office of Pers. Mgmt., to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 23, 2015, 10:07 p.m.) at HOGR020316-000288 (OPM Production: Feb. 16, 2016).

was published without apparently verifying all the facts surrounding the story and CyTech's role in incident response and forensic support.[763]

OPM Description of CyTech's Role Was Misleading

Testimony and public statements by OPM officials regarding CyTech's role in the data breach incident response and forensic support activities from April to May 2015 were confusing and misleading. OPM was also slow to respond to document production requests regarding this issue further compounding the confusion. When OPM produced documents in early 2016 and as the investigation proceeded, the CyTech narrative became clear. However, when the CyTech story was first reported in June 2015, the details were less than clear and further confused by senior OPM officials' testimony. In June 2015, the CyTech story was the subject of various press reports, including the June 10, 2015 story in the *Wall Street Journal*. On June 16, 2015, former OPM Director Katherine Archuleta testified before the Committee that "OPM detected the intrusion" and denied that contractors did so.[764] Archuleta omitted the fact that Cylance and CyTech played critical roles in identifying the actual malware and providing forensic support.

Archuleta and Seymour Provided Misleading Testimony to Committee

On June 23, 2015, the House Permanent Select Committee on Intelligence (HPSCI) referred evidence to the Committee obtained from CyTech.[765] In light of the press developments and the information from HPSCI, Rep. Turner questioned Seymour and Archuleta about CyTech when they appeared before the Committee on June 24, 2015.[766]

Rep. Mike Turner (R-OH) questions Archuleta and Seymour at June 23, 2015 Committee hearing

---

[763] Email Jackie Koszczuk, Dir. of Comm., U.S. Office of Pers. Mgmt., to Damian Paletta, Reporter, Wall St. J. (June 10, 2015, 7:15 p.m.) at HOGR020316-000159 (OPM Production: Feb. 16, 2016). The WSJ declined to print a retraction "solely on the basis of the agency's assertion that it is inaccurate." Email from Robert Ourlian, News Editor, Wall St. J., to Jackie Koszczuk, Dir. of Comm., U.S. Office of Pers. Mgmt. (June 10, 2015, 9:26 p.m.) at HOGR020316-00163 (OPM Production: Feb. 16, 2016).

[764] *OPM Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (June 16, 2015) (statement of Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt.).

[765] The House Permanent Select Committee on Intelligence also referred information related to the CyTech matter to the Committee. Letter from the Hon. Devin Nunes, Chairman and the Hon. Adam Schiff, Ranking Member, H. Perm. Select Comm. on Intelligence to the Hon. Jason Chaffetz, Chairman and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (June 23, 2015).

[766] *Hearing on OPM Data Breach: Part II.*

Rep. Turner asked Archuleta and Seymour: "was CyTech involved in the discovery of this data breach?" Both witnesses responded no, CyTech was not involved.[767] Documents and testimony do show OPM identified and reported to US-CERT on April 15, 2015 that an unknown Secure Sockets Layer (SSL) certificate was beaconing to a site (opmsecurity.org) not associated with OPM.[768] OPM officials left out the fact that Cylance and CyTech also identified malware related to the data breach. In the case of CyTech, CyFIR agents were deployed on April 21, 2015 to several production servers where CyFIR images were collected and transmitted to US-CERT. Subsequent analysis showed the presence of malicious files related to the data breach.[769]

Rep. Turner also asked Archuleta and Seymour whether Cytech was ever brought in to run a scan on OPM's equipment.[770] Seymour testified that "CyTech was engaged with OPM" and added that OPM was looking at using CyTech's tool on the OPM network.[771] She stated her understanding was that OPM "gave them some information to demonstrate whether their tool would find information on [OPM's] network, and that – in doing so, they did indeed find those indicators on OPM's network."[772] She testified:

Seymour: [W]e had purchased licenses for CyTech's tool. We wanted to see if that tool set would also discover what we had already discovered. So, yes, they put their tools on our network, and yes, they found that information as well."

Turner: So you were tricking them? You like already knew this, but you brought them in and said, Shazam, you caught it too? That seems highly unlikely, don't you think?

Seymour: We do a lot of research before we decide on what tools we are going to buy for our network.

Turner: At that point you hadn't removed the system from your system? I mean, you knew it was there, you brought them in, and their system discovered it too, which means it would have been continuously running, and that personnel information would have been still at risk. Correct?

Seymour: No, Sir. We had latent malware on our system that we were watching that we had quarantined.

---

[150] *Id.*
[768] AAR Timeline – Unknown SSL Certificate (April 15, 2015), at HOGR020316-1922 (OPM Production: Apr. 29, 2016).
[769] U.S. Dep't of Homeland Security/US-CERT, Preliminary Digital Media Analysis-INC465355-A (May 4, 2015) at HOGR0724-001032 (OPM Production: Dec. 22, 2015); Briefing by U.S. Office of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Apr. 18, 2016).
[770] *Hearing on OPM Data Breach: Part II.*
[771] *Id.*
[772] *Id.*

Turner: You had quarantined it. So it was no longer operating.

Seymour: That is correct.[773]

Seymour's testimony raised several questions. First, documents show OPM had not purchased licenses, or anything else, from CyTech—despite a verbal request for an emergency purchase order.[774]

Second, testimony obtained by the Committee shows CyTech was not given the indicators of compromise prior to running CyFIR on OPM's network on April 21, 2015. Documents obtained from OPM suggest indicators of compromise were shared with an OPM contractor Imperatis – on April 23, 2015 days after the April 21 CyTech demonstration.[775] An Imperatis employee escorted Cotton when he was onsite at OPM, but there is no evidence showing he provided Cotton or CyTech with indicators of compromise prior to the April 21 demonstration.

Third, Seymour's claim that the CyFIR tool identified "latent malware" on systems that had been quarantined is not accurate. Wagner testified the CyFIR tool was deployed in a live production environment.[776] Documents show OPM prioritized deployment of the CyFir tool to servers in the OPM production environment.[777] In fact, the CyFIR tool is designed to run in a live environment and runs against programs running in live memory.[778]

Seymour's claim that the malware in the OPM system had been quarantined is not accurate. Cotton testified: "there was no quarantine in place when I found the malware live on the system on the morning of the 22nd."[779] The agency did not move the primary tool used to identify malware enterprise-wide (CylanceProtect) from alert to auto-quarantine mode until April 24, 2015.[780] The CyFIR tool did in fact identify malware, and contrary to Seymour's testimony, the CyFIR tool did so in a live environment.[781]

Data on CyTech's CyFIR Appliance Collected During the 2015 Incident Response Period was Deleted

After two hearings in June 2015, the Committee requested additional information and documents from OPM related to the data breach incident announced in 2015, including specific

---

[773] *Hearing on OPM Data Breach: Part II* (Statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).
[774] Wagner Tr. at 103.
[775] Cotton Tr. at 14, 16; Email from Brendan Saulsbury, Senior Cyber Security Engineer, SRA, to [redacted] Imperatis (April 23, 2015, 12:47 p.m.) at HOGR020316-000254 (OPM Production: Feb. 16, 2016) ([redacted] escorted Cotton for the April 21 demonstration).
[776] Wagner Tr. at 103.
[777] Message from [redacted] Contractor, U.S. Office of Pers. Mgmt., to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Apr. 28, 2015) at HOGR020316-000333 (OPM Production: Feb. 16, 2016).
[778] Cotton Tr. at 10.
[779] Cotton Tr. at 77.
[780] Saulsbury Tr. at 71; *see also* McClure Tr., Ex. 12.
[781] Wagner Tr. at 102.

information about CyTech and the use of the CyFIR tool at OPM. The Committee requested information about CyTech's role in this incident in a July 24, 2015 letter to OPM, then Chairman Chaffetz issued a preservation order to OPM on August 21, 2015, and on September 9, 2015, the Committee requested specific additional information about CyTech's tool, CyFIR, after learning data on the tool was deleted before it was returned to CyTech.[782]

Despite a clear obligation to preserve documents and evidence relevant to the Committee's investigation, OPM deleted data on CyTech's CyFIR appliance before returning the appliance to CyTech on August 20, 2015. The CyFIR appliance was used to collect forensic images that would assist the investigation of the data breach. Those images are relevant to determining the scope of the intrusion and data exfiltration.

OPM Retained CyTech's CyFIR Appliance Through August 2015

On June 23, 2015, HPSCI advised the Committee that OPM was still in possession of the CyFIR appliance.[783] Documents show that on June 25, 2015, OPM requested instructions from CyTech to "uninstall" the CyFIR agents.[784] CyTech subsequently requested that the CyFIR appliance be returned, but it was not returned until August 20, 2015—one day after Committee investigators visited CyTech's offices.[785]

In mid-August 2015, OPM deleted data on the CyFIR appliance and arranged to return it. On August 13, 2015, Imperatis, the OPM contractor that introduced CyTech to OPM, wrote Wagner and advised that CyTech wanted the CyFIR appliance and offered to help coordinate its return.[786] An OPM contractor who worked for Wagner on IT Security Operations wrote: "we need to scrub HDs [hard drives] prior to pick up."[787]

Before Returning the CyFIR Appliance OPM Deleted Key Data.

After some internal discussion about the best way to remove "sensitive OPM data" from the CyFIR appliance, Saulsbury and Tonda, two OPM IT security operations contract employees handling security operations, requested permission to "secure delete all sensitive OPM data from the CyFIR demo server including memory images, disk images, and any individual files or

---

[782] Letter from the Hon. Jason Chaffetz, Chairman and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (July 24, 2015); Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform and the Hon. Michael Turner, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Sept. 9, 2015).

[783] Letter from the Hon. Devin Nunes, Chairman and the Hon. Adam Schiff, Ranking Member, H. Perm. Select Comm. on Intelligence, to the Hon. Jason Chaffetz, Chairman and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (June 23, 2015).

[784] Cotton Tr., Ex. 6 (Email from [redacted] Contractor, U.S. Office of Pers. Mgmt., to Juan Bonilla, Senior Sec. Consultant, CyTech (June 25, 2015).

[785] Cotton Tr. at 72.

[786] Email from Patrick Mulvaney, Imperatis, to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Aug. 13, 2015, 11:26 a.m.) at HOGR0909-000080-81 (OPM Production: Oct. 28, 2015).

[787] Email from Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt., to Patrick Mulvaney, Imperatis, and Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Aug. 13, 2015, 11:41 a.m.) at HOGR0909-000080-81 (OPM Production: Oct. 28, 2015).

metadata extracted from OPM devices."[788] On August 17, 2015, Wagner approved this request.[789]

The process of deleting the data was tedious. On August 18, 2015, Saulsbury—who had been directed to delete the data on the CyFIR appliance—reported to his colleague Tonda that the "secure delete is only about 30% complete."[790] Saulsbury and Tonda were aware that the Committee was investigating the breach at this time. In an email, Saulsbury asked Tonda, "do you need help with anything for the HOGR stuff."[791] Tonda responded: "[N]ot yet. I'm reviewing it with Jeff now. Maybe later." So at the same time, the data on the CyFIR appliance was being deleted, they were aware that there were outstanding Committee requests for information. Nonetheless, OPM made the decision to delete the data on the CyFIR appliance.[792]

On August 19, 2015 (the same day that Committee investigators met with CyTech staff at their offices), a counsel from the OPM OIG told staff in the Office of General Counsel that CyTech was "complaining that OPM still has not returned the server/application thingee that CyTech built and left with OPM after the demonstration."[793] He further stated: "heard something that will create unpleasant work for both our offices unless it's headed off. . . . looks like a bad-publicity lawsuit coming down the pike unless, assuming of course that OCIO has it, OPM returns it. Just saying . . ."[794] Wagner forwarded this exchange to an Imperatis employee and said, "I want this [CyFir appliance] gone today."[795]

There is no evidence showing any OPM official recommended that the data on the CyFIR appliance should be preserved in light of the ongoing congressional investigation.

After the CyFIR appliance was returned on August 20, 2015, CyTech examined the appliance to determine what data was on the appliance for the purpose of responding to the Committee's requests for information. CyTech determined that 11,035 files and directories were deleted by OPM personnel or contractors on August 17, 18, and 19, 2015.[796] Cotton testified that

---

[788] Email from Brendan Saulsbury, Senior Cyber Security Engineer, SRA, to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. and Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (Aug. 17, 2015) at HOGR0909-000107 (OPM Production: Oct. 28, 2015).

[789] Email from Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Aug. 17, 2015, 2:00 p.m.) at HOGR0909-000107 (OPM Production: Oct. 28, 2015).

[790] Messages between Brendan Saulsbury and Jonathan Tonda, OPM IT Security Operations contractors (Aug. 18, 205) at HOGR0909-000151-52 (OPM Production: Oct. 31, 2015).

[791] *Id.*

[792] Email from Jeff Wagner, Dir. IT. Sec. Operations, U.S. Office of Pers. Mgmt. to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Aug. 17, 2015, 2:00 p.m.) at HOGR0909-000107 (OPM Production: Oct. 28, 2015).

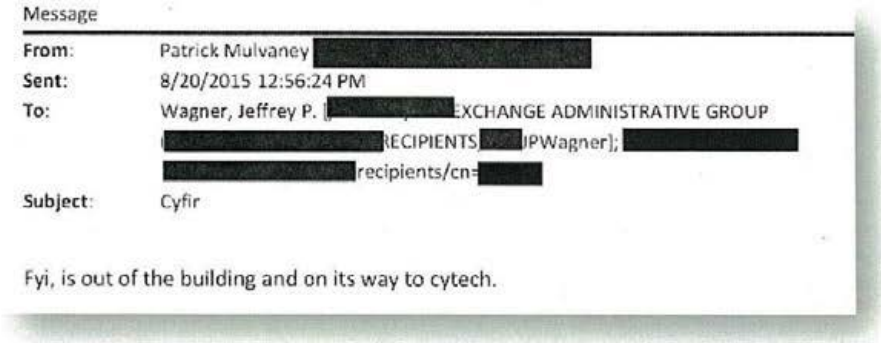
[793] Email from OIG Counsel, U.S. Office of Pers. Mgmt., to Associate Gen. Counsel, U.S. Office of Pers. Mgmt. (Aug. 19, 2015, 1:27 p.m.) at HOGR0909-000522 (OPM Production: Oct. 28, 2015).

[794] Email from OIG Counsel, U.S. Office of Pers. Mgmt., to Associate Gen. Counsel, U.S. Office of Pers. Mgmt. (Aug. 19, 2015, 1:27 p.m.) at HOGR0909-000522 (OPM Production: Oct. 28, 2015).

[795] Email from Jeff Wagner, Dir. IT. Sec. Operations, U.S. Office of Pers. Mgmt. to Patrick Mulvaney, Imperatis and Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Aug. 19, 2015, 6:03 p.m.) at HOGR0909-000523 (OPM Production: Oct. 28, 2015).

[796] Cotton Tr., Ex. 12 (Forensics Report: OPM CyFIR Server Analysis Report (Sept. 10, 2015)). The Forensics Report included a 600 page Appendix A that listed in detail the 11,035 file names and any data or artifacts related to those files that was recoverable. Cotton Tr. at 74-75.

when CyTech examined the CyFIR device, they were interested in recovering certain database information in order to answer the Committee's questions and to provide clarity as to the scope of their activities while onsite at OPM in April-May 2015.[797] Cotton stated: "the CyFIR tool was not in a functioning state when it was returned to us."[798] Cotton also testified that the information on the CyFIR server would have been covered by the Committee's August 21, 2015 preservation order.[799]



Message

From: Patrick Mulvaney [redacted]

Sent: 8/20/2015 12:56:24 PM

To: Wagner, Jeffrey P. [redacted] EXCHANGE ADMINISTRATIVE GROUP [redacted] RECIPIENTS [redacted] JPWagner]; [redacted] recipients/cn=[redacted]

Subject: Cyfir

Fyi, is out of the building and on its way to cytech.

OPM "Sanitized" the CyFIR Appliance

On October 28, 2015, OPM responded to the Committee's September 9, 2015 request for information about the CyFIR appliance.[800] The agency disclosed they "sanitized" the CyFIR appliance prior to returning it to CyTech.[801] The agency stated it did so in accordance with best practices and applicable information security policies[802]—without regard for the ongoing congressional investigation. The agency knew as of July 24, 2015 that there was an ongoing congressional investigation, and that CyTech's role in the data breach incident was a subject of the investigation.[803] Further, the Committee issued a preservation order related to the investigation on August 21, 2015.[804] The agency deleted the data on the appliance between August 17 and19, 2015.

---

[797] Cotton Tr. at 73.
[798] Cotton Tr. at 74.
[799] Cotton Tr. at 106.
[800] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform and the Hon. Michael Turner, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Sept. 9, 2015); Letter from the Hon. Beth Cobert, Acting Dir. U.S. Office of Pers. Mgmt. to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform and the Hon. Michael Turner (Oct. 28, 2015).
[801] Letter from the Hon. Beth Cobert, Acting Dir. U.S. Office of Pers. Mgmt. to the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform and the Hon. Michael Turner (Oct. 28, 2015).
[802] *Id.*
[803] Letter from the Hon. Jason Chaffetz, Chairman and the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (July 24, 2015).
[804] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform to the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. (Aug. 21, 2015).

OPM Violated the Anti-Deficiency Act

Documents and testimony show CyTech provided a service to OPM and OPM did not pay for this service. The Anti-deficiency Act (ADA) prohibits a federal agency from accepting voluntary services without obtaining an agreement in writing that the contractor will never seek payment.

The ADA's prohibition on accepting voluntary services

The ADA generally does not permit a federal agency or department to accept services from a contractor free of charge. The relevant section of the ADA states:

> An officer or employee of the United States Government or of the District of Columbia government may not accept voluntary services for either government or employ personal services exceeding that authorized by law except for emergencies involving the safety of human life or the protection of property.[805]

The ADA was enacted to prevent the use of voluntary services to avoid congressional scrutiny. The ADA, first passed in 1884 and substantially amended in 1950 and 1982, represented a desire to set strict limits on executive branch payroll and procurement officials.[806] Executive branch employees often worked overtime in excess of the agency's congressionally approved budgets, and the agency would subsequently request back pay for the employees.[807] Congress found it politically and morally problematic to deny payment to individuals who had rendered valuable services to the federal government—a fact the agencies well knew.[808] To eliminate this tactic for increasing departmental budgets, Congress prohibited voluntary services altogether.

The "gratuitous" services exception

While "voluntary" services are prohibited by the ADA, courts have distinguished "voluntary" services from "gratuitous" services. "Gratuitous" services are offered under an arrangement in which the government receives uncompensated services in accordance with an advance written agreement or contract in which the provider of the services agrees to serve without compensation.[809]

A contractor or individual can thus provide "gratuitous" services free of charge without violating the ADA so long as the contractor signs a written agreement in advance stating that the

---

[805] 31 U.S.C. § 1342 (2012).
[806] *See* Gov't Accountability Office, B-309301, *Recess Appointment of Sam Fox* (June 8, 2007).
[807] *Id.*
[808] *Id.*
[809] *Id.*

services are being offered without expectation of payment and waiving any future pay claims against the government.[810]

The "emergencies" exception

The ADA allows the federal government to benefit from personal services exceeding what is authorized by law in the event of "emergencies involving the safety of human life or the protection of property."[811]

The exception has historically been understood to require two factors in order to be invoked: (1) a "reasonable and articulable connection between the function to be performed and the safety of human life or the protection of property," and (2) "some reasonable likelihood that the safety of human life or the protection or property would be compromised, in some degree, by delay in the performance of the function in question."[812]

Previous successful invocations of the emergency exception have required a close nexus between the service being provided and the life or property protected. For example, the arbiter of ADA violations, the Government Accountability Office, found an exception when a municipal health officer disinfected a federal government compound to prevent the further spread of diphtheria that had already resulted in four deaths in that specific compound.[813]

When the service provided is merely convenient or helpful in avoiding a future emergency, it does not qualify under the exception. GAO ruled in 1930 that a man who offered to tow a Navy seaplane to a nearby island after a forced landing did not qualify under the emergency exemption.[814] GAO found the rendering of service to avoid a potential future emergency was not enough to invoke the exception.[815]

The ADA applied to the OPM and CyTech Situation

On April 21, 2015, CyTech provided a demonstration of its CyFIR tool at OPM's facility in Washington, D.C.[816] CyTech CEO Ben Cotton conducted the demonstration using CyTech equipment, most notably a computer forensics tool known as CyFIR.[817] For the demonstration, CyTech brought a CyFIR server to OPM, which would be connected to OPM's network and provide forensics services on up to twenty machines.[818]

---

[810] Gov't Accountability Off., B-324214, Decision, *Department of Treasury—Acceptance of Voluntary Services* (Jan. 27, 2014).
[811] 31 U.S.C. § 1342 (2012).
[812] 43 Op. Att'y Gen. 293, 302 (1981).
[813] 12 Com. Dec. 155 (Gov't Accountability Office 1905).
[814] 10 Com. Gen. 248 (Gov't Accountability Office 1930).
[815] 10 Com. Gen. 248 (Gov't Accountability Office 1930).
[816] OPM Visitor Log, Washington, D.C. (Apr. 21, 2015) at HOGR020316-000522 (OPM Production: Feb. 16, 2016).
[817] Email from [redacted] Imperatis, to Jeff Wagner, Dir. Info. Tech. Sec. Operations and Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (Apr. 20, 2015, 4:22 p.m.) at HOGR0909-000007 (OPM Production: Oct. 28, 2015).
[818] Cotton Tr. at 43.

CyTech expected to be paid

At that time, OPM had not purchased any licenses from CyTech. CyTech only provided a limited licensing arrangement for the purposes of the demonstration (for which typically there is no expectation of payment), to enable the installation of the CyFIR tool on twenty OPM machines for thirty days, thereby allowing the machines to be scanned for malware and unknown software processes. On April 22, 2015, Cotton reported the results of the demonstration to OPM staff and to [redacted] of Imperatis, another contractor retained by OPM.[819] The CyTech system had identified three unknown processes.[820] The results of the CyFIR scan were copied to a thumb drive and taken to OPM's security experts.[821]

Around noon that day, Cotton had a conversation with Jeff Wagner, OPM's Director of IT Security Operations, about the CyFIR findings. Wagner asked for a purchase order for the CyFIR tool that would cover 15,000 agents, six appliances, and 1,000 data analysts.[822] Cotton agreed to immediately expand the number of CyFIR licenses to 1,000 before a purchase order was formalized.[823] In this conversation with Wagner, Cotton also committed a CyTech expert to provide incident response and forensic support for the investigation.[824]

OPM's purchase order for CyTech services was to be made via a preexisting contract vehicle with Imperatis.[825] Consequently, Cytech provided a quote to Imperatis on April 24 for 15,000 CyFIR licenses, six CyFIR appliances, six training vouchers, and 1,040 onsite engineering support hours that would cost a total of $818,000.[826] In the meantime, CyTech, relying on the government's verbal request for services beyond a typical demonstration situation, began expanding its services to OPM and provided a license to OPM on April 22, 2015 for 1,000 endpoints that expired on June 30, 2015.[827]

The documents show specific incident response and forensic support activities that CyTech provided to OPM for which OPM should have compensated CyTech. The documents show OPM confirmed that the CyTech expert, Juan Bonilla, would be "assisting with an investigation over the next two weeks."[828] In terms of specific CyTech activities, Cotton

---

[819] Wagner Tr. at 102-103.
[820] Wagner Tr. at 102-103.
[821] Cotton Tr. at 19.
[822] Cotton Tr., Ex. 3, 4 (CyTech Price Quote ($818,000) for Emergency Purchase Order (Apr. 24, 2015) and CyTech [redacted] Transmittal email to Imperatis for CyTech Quote (Apr. 24, 2015)).
[823] Email from Ben Cotton, Chief Exec. Officer, CyTech to H. Comm. on Overisght & Gov't Reform Majority Staff (Apr. 16, 2016) (confirming the nature of the licensing arrangement as of April 22, 2015) (on file with the Committee).
[824] Cotton Tr. at 25. Cotton noted that CyTech's expert, Bonilla, as a senior member of the CyTech team, is typically billed at between $350 and $450 an hour. *Id.*
[825] Cotton Tr. at 23.
[826] Cotton Tr., Ex. 3, 4 (CyTech Price Quote ($818,000) for Emergency Purchase Order (Apr. 24, 2015) and CyTech [redacted] Transmittal email to Imperatis for CyTech Quote (Apr. 24, 2015)).
[827] Email from Ben Cotton, Chief Exec. Officer, CyTech to H. Comm. on Overisght & Gov't Reform Majority Staff (Apr. 16, 2016) (confirming the nature of the licensing arrangement as of April 22, 2015) (on file with the Committee).
[828] Email Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. to IT Administration, U.S. Office of Pers. Mgmt. (Apr. 28, 2015) at HOGR020316-000707 (OPM Production: Feb. 16, 2016).

testified that CyTech was initially asked to image all the random access memory of about fifty computers and then image the hard drives for those computers and pull event logs for OPM.[829] CyTech also worked with Cylance, an OPM contractor, to fulfill their requests for files.[830]

Documents show CyTech's role in providing forensic support was significant—CyTech collected thousands of images in its forensic support role.[831] Documents show the agency continued to use the CyFIR tool in May 2015 through early June. For example, on May 7, 2015, Cylance requested deploying CyFIR to a particular OPM host machine.[832] In another email on June 1, 2015, an OPM contractor confirmed that "all other security agents are currently running, Cylan[c]e, CyFIR, Forescout . . . ."[833]

Documents show the agency and its contractor, Imperatis, expected OPM would be compensating CyTech for incident response and forensic support based on the conversations CyTech had with OPM in April 2015. For example, during the week of April 27, 2015, an Imperatis weekly report stated: "coordinating equipment installation and configuration with security vendors" including "working to finalize BOM [bill of materials]" for CyFIR.[834] Then, as late as June 5, 2015, Imperatis inquired about the status of the CyTech quote. An Imperatis employee emailed an OPM official: "do you want CyFIR for the existing network, I assume yes to compliment [*sic*] your Encase tool?"[835]

The documents show CyTech provided a demonstration, and following that demonstration, OPM requested a purchase order for CyTech services to support incident response activities, including forensic support. Based on the agency's apparent intent to finalize a purchase order, CyTech expanded the CyFIR licensing arrangement beyond what would normally be provided in a demonstration and provided onsite incident response services from April 23 through May 1, 2015. OPM also retained the CyFIR equipment for months after the demonstration, and used at least some of the licenses for CyFIR.[836] The record demonstrates CyTech was never compensated for these services and CyTech did not sign an agreement stipulating that its services would be provided for free.

---

[829] Cotton Tr. at 27-28.
[830] Email from Chris Coulter, Managing Dir., Cylance, to Ben Cotton, Chief Exec. Officer, CyTech (Apr. 24, 2015, 5:54 p.m.) at HOGR020316-000010 (OPM Production: Feb. 16, 2016).
[831] Email from Juan Bonilla, Senior Sec. Consultant, CyTech, to Brendan Saulsbury, Senior Cyber Security Engineer, SRA (Apr. 29, 2015, 5:26 p.m.) at HOGR020316-000043 (OPM Production: Feb. 16, 2016).
[832] Email from Chris Coulter, Managing Dir., Cylance, to Jonathan Tonda, Contractor, U.S. Office of Pers. Mgmt. (May 7, 2015, 3:56 p.m.) at HOGRO020316-000351 (OPM Production: Feb. 16, 2016).
[833] Email from Contractor, U.S. Office of Pers. Mgmt. to U.S. Office of Pers. Mgmt. Employees (June 1, 2015, 4:42 p.m.) at HOGR020316-000363 (OPM Production: Feb. 16, 2016).
[834] Imperatis Weekly Report (Apr. 27, 2015-May 1, 2015), Attach. 6 at 000758 (Imperatis Production: Sept. 1, 2015).
[835] Email from Patrick Mulvaney, Imperatis to Jeff Wagner, Dir. Info. Tech. Sec. Operations, U.S. Office of Pers. Mgmt. (June 5, 2015, 8:51 p.m.) at HOGR0909-000046 (OPM Production: Oct. 28, 2015).
[836] *See* Email from Contractor, U.S. Office of Pers. Mgmt. to U.S. Office of Pers. Mgmt. Employees (June 1, 2015, 4:42 p.m.) at HOGR020316-000363 (OPM Production: Feb. 16, 2016). (OPM contractor listing CyFIR as a security tool running on an OPM server); *see also* List of Locations on which CyTech's CyFIR was Tested at HOGR0724-000320-321 (OPM Production Sept. 25, 2015).

The ADA prohibits a transaction of this nature. All the services that were unrelated to the product demonstration—including the provision of 1,000 additional licenses after the demonstration was over—should have been paid for. The agency also kept CyTech's CyFIR hardware for months after the demonstration. CyTech did not sign any written agreement that might have converted its voluntary services to gratuitous services because it expected to eventually receive payment.

This scenario raises the same concerns that the authors of the ADA had in mind when the bill was originally passed. The agency accepted a valuable service from a company that expected to be paid, but never was. The agency's actions placed the federal government in the uncomfortable position of either approving retroactive payment for voluntary services, or forcing CyTech—a small, disabled veteran owned business—to bear the sole burden for thousands of dollars in expenses incurred in good faith to help OPM respond to a significant cyber incident.

Chapter 6: Connections Between the 2014 and 2015 Intrusions

There has been significant public commentary on the source of the data breaches at OPM.[837] The Administration has "chosen not to make any official assertions about attribution."[838] Some Administration officials have hinted at the source behind the cyberattacks. Director of National Intelligence James Clapper has referred to China as "the leading suspect," stating "you have to kind of salute the Chinese for what they did."[839]

The documents and testimony gathered over the course of the investigation, as well as analysis of private sector threat research, show the data breaches discovered in 2014 and 2015 are likely connected, potentially coordinated campaigns by two threat actor groups. This conclusion is based on evidence that indicates the threat actors' "tactics, techniques, and procedures" (TTPs) and attack infrastructure share a common source or benefactor.

The documents show a broader campaign against federal workers associated with the hacking collective Axiom Threat Actor Group ("Axiom") and the threat actor Deep Panda. This conclusion is based on a multifactor analysis of the threat actors, and the tools they used to perpetrate the data breaches in 2014 and 2015:

- First, the data breach discovered in March 2014 was likely conducted by Axiom, based on the presence of Hikit malware and other TTPs associated with this group.

- Second, the data breach discovered in April 2015 was likely perpetrated by the group Deep Panda (a.k.a. Shell_Crew; a.k.a. Deputy Dog) as part of a broader campaign that targeted federal workers. This conclusion is based on commonalities in the 2015 adversary's attack infrastructure and TTPs common to other hacks attributed to Deep Panda, including attacks on Wellpoint/Anthem, VAE Inc., and United Airlines. However, the cyber intrusion and data theft announced by Anthem in 2015 is a separate

---

[837] Brian Krebs, *Catching Up on the OPM Breach,* KREBS ON SECURITY (June 15, 2015, 11:25 AM), available at: http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/; *see also* Ellen Nakashima, *U.S. Decides Against Publicly Blaming China for Data Breach*, WASH. POST, July 21, 2015, available at: https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html.

[838] Ellen Nakashima, *U.S. Decides Against Publicly Blaming China for Data Breach*, WASH. POST, July 21, 2015, available at: https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html (citing a Senior Administration Official).

[839] David Welna, *In Data Breach, Reluctance to Point the Finger at China*, NAT'L PUB. RADIO, July 2, 2015, http://www.npr.org/sections/parallels/2015/07/02/419458637/in-data-breach-reluctance-to-point-the-finger-at-china. Director Clapper's nod towards China as the perpetrator of the OPM data breaches gained credibility when the Chinese government arrested "a handful of hackers it says were connected with the breach." Ellen Nakashima, *Chinese Government Has Arrested Hackers it Says Breached OPM Database*, WASH.POST, Dec. 2, 2015, available at: https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html.

attack by a separate threat-actor group unrelated to the hack against OPM discovered in 2015.

- Third, both Axiom and Deep Panda are believed to be state-sponsored threat-actors supported by the same foreign government.[840]

- Fourth, based on these facts, the Committee finds that the 2014 and 2014/2015 cyber intrusions into OPM's networks were likely connected, possibly coordinated campaigns.

One Group, Several Names

There is an inherent challenge in associating a data breach to a particular hacking group, as threat researchers and governments do not have a common naming convention for cyber threat actors.[841]

Threat intelligence researchers generally name threat actor groups based on intrusions—called campaigns—that share common characteristics. Over time, analyses of campaigns performed by different firms may result in the same threat actor group being given multiple different names. Only later are these different names linked or identified as the same group. The groups that will be discussed in this report—Axiom, Deep Panda, Shell_Crew, Deputy Dog, APT6, etc.—were created by threat researchers. For instance, Crowdstrike researchers have relied on the naming convention of "Deep Panda" [842] while other groups term the same threat actor groups as: PinkPanther, Deputy Dog, Shell_Crew, APT17, Group 72, Black Vine, etc.[843]

Finally, because naming conventions of threat actors often revolve around intrusion campaigns rather than membership and affiliation, the analysis is unable to account for major changes to the threat actor group's membership, funding, TTPs, malware, or infrastructure over time. This may result in one group being misidentified as another or two actor groups being identified as one.

---

[840] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 8-9.

[841] See e.g. Brian Krebs, *Catching Up on the OPM Breach,* KREBS ON SECURITY (June 15, 2015, 11:25 AM), available at: http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/; Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 8-9; ThreatConnect Research Team, OPM Breach Analysis, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/.

[842] Dmitri Alperovitch, Deep in Thought: Chinese Targeting of National Security Think Tanks, CROWDSTRIKE BLOG (July 7, 2014), http://www.crowdstrike.com/blog/deep-thought-chinese-targeting-national-security-think-tanks/.

[843] *DeepPanda or Shell Crew: Who is Behind the Cyber Attacks on US Networks*, RESEARCH MOZ (June 22, 2015), http://www.researchmoz.us/article/deeppanda-or-shell-crew-who-is-behind-the-cyber-attacks-on-us-networks; RSA Incident Response, *Emerging Threat Profile Shell Crew* 5 (Jan. 2014),https://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf. Note: A set of common characteristics in these groups' cyber campaigns and intrusions led to the belief that they are all actually the same group with several different names.

The 2014 Data Breach: The Unique Malware of the Axiom Group

The Axiom Group has been found responsible for a series of highly sophisticated cyber campaigns against public and private sector targets throughout the world in the last six years.[844] The definitive technical and behavioral report on Axiom's history and methods of attack was conducted by the threat research group at Novetta in 2014,[845] which found, in part, that the "Axiom threat group is a well-resourced, disciplined, and sophisticated subgroup of a larger cyber espionage group."[846]

The data breach at OPM in 2014, like other attacks perpetrated by Axiom, or one of its subgroups, involved the use of Hikit malware as the primary means of maintaining presence in OPM's environment.[847] **According to Novetta, Hikit malware is a "tool only seen used by Axiom."**[848]

Hikit malware is a sophisticated remote access tool (RAT) that offers attackers the ability to create covert backdoors into target computer networks and eventually take full control of target computer networks.[849] Hikit is purposefully built to evade detection and circumvent protections offered by firewalls and network monitoring tools.[850]

Similar to most sophisticated cyber intrusion campaigns, Hikit can be modified for tailored-use in a target's network, and optimized to operate within and take advantage of the vulnerabilities of the software, hardware, or operating system in the victim's environment.[851] Additionally, configuration files extracted to Hikit binaries indicate that command and control domains (C2) callbacks are tailored towards the geographic and network environment in which the target network is located. According to Novetta, "C2 domains will consistently be named and hosted in such a way that traffic appears legitimate, likely in an effort to fool network security operators of target organizations."[852]

DHS' OPM Incident Report from June 2014 positively identified the malware responsible for the 2014 intrusion as two variants of Hikit: Hikit A and Hikit B.[853] Hikit A and Hikit B differ primarily in the methods they use to communicate with their C2 servers. Hikit A uses a "unique 4-byte XOR key for each packet" while Hikit B "compresses its network traffic

---

[844] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 8-9.
[845] Novetta and the Cyber Security Coalition that conducted "Operation SMN" published an executive summary of the operation on October 15, 2014. The final report was released in November 2014 and is the product of an industry led effort to identify and disrupt a threat actor group.
[846] Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 4.
[847] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Jeffrey P. Wagner (Feb. 18, 2016) at 31-32.
[848] Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 19.
[849] Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 28.
[850] Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 24-25.
[851] Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 4, 21. The Novetta report makes many references to HiKit customization by the Axiom group, and consider it a "tier 1" custom piece of malware. *Id.* at 4, 21.
[852] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 21.
[853] June 2014 OPM Incident Report at HOGR0818-001234.

with quicklz then it is XORed with a hash of 'matrix_password' concatenated with itself in a loop six times."[854]

The actors responsible for the 2014 intrusion used a wide variety of command and control servers (C2) throughout the entirety of the intrusion lifecycle.[855] Forensic investigators were able to identify C2 servers active and in use during 2014 by detailed, deep inspection of network traffic in and out of OPM's environment. Analysis of the Hikit malware used in the attack provided a granular, comprehensive picture of the command and control infrastructure that was created to support the campaign. The domains and IP addresses were hard-coded as call-back functions within the Hikit malware used in the campaign.

Hostname	IP Address	Hikit Variant	Function	C2 Domain	Previous
[redacted]	[redacted]	Hikit A	Bandwidth Monitoring Server	lgemetic[.]suroot[.]com	[redacted]
[redacted]	[redacted]	Hikit A	[redacted] Server	bookservice[.]chatnook[.]com	[redacted]
[redacted]	[redacted]	Hikit A	Backup [redacted] Storage Manager	testimagecdn[.]servepics[.]com	[redacted]
[redacted]	[redacted]	Hikit A	[redacted] Network Performance Monitor	testimagecdn[.]servepics[.]com	[redacted]
[redacted]	[redacted]	Hikit A	[redacted] Server	testimagecdn[.]servepics[.]com	[redacted]
[redacted]	[redacted]	Hikit A	[redacted]	N/A	[redacted]
			Server		
[redacted]	[redacted]	Hikit B	[redacted] Server	www[.]maxcdns[.]com	[redacted]
[redacted]	[redacted]	Hikit B	[redacted] Server	www[.]edjecasts[.]com	[redacted]
[redacted]	[redacted]	Hikit B	[redacted] Server	statics[.]hopto[.]org	[redacted]

C2 Domains and IPs used in the 2014 intrusion and their associated Hikit malware counterparts[856]

Hikit malware is extremely unique to a specific threat actor group. Hikit is known as a "Tier 1" implant, which means that it is a custom piece of malware that can be strongly attributed to one particular threat actor group.[857] Axiom uses a variety of tools in varying stages of the intrusion cycle, which fall generally into four families: "These families of malware range in uniqueness from extremely common (Poison Ivy, Gh0st, ZXshell) to more focused tools used by

[854] *Id.*
[855] June 2014 OPM Incident Report at HOGR0818-001244 - 1245.
[856] June 2014 OPM Incident Report at HOGR0818-001244 - 1245.
[857] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 19.

Axiom and other threat groups directed by the same organization (Derusbi, Fexel) to tools only seen used by Axiom (ZoxPNG/ZoxRPC, Hikit)."[858]

The use of Hikit in the 2014 intrusion strongly indicates that a group associated with Axiom is responsible for the 2014 intrusion. Analysis by open-source threat researchers is consistent with this finding, attributing the attack to a state-sponsored actor;[859] the Novetta report highlights that the Axiom Group's targets – Asian and Western governments responsible for government records, journalists and media organizations, et. al.[860]

Hikit was first detected in 2011 and has evolved and developed into multiple versions since then.[861] Hikit splits into two generational variants: Hikit generation one, which dates back to 2011, and Hikit generation 2, which spans between 2011 and 2013.[862] Both generations of Hikit allow a great deal of functionality for threat actors. Once Hikit is dropped on a system, the attacker will have a variety of capabilities, including:

1. File management (upload and download).

2. Remote shell.

3. Network tunneling (proxying).

4. *Ad hoc* network generation (connecting multiple Hikit infected machines to create a secondary network on top of the victim's network topology).[863]

In addition to there being two generations of Hikit, there are also variants. All the malware found in 2014 were two variants of Hikit malware, termed Hikit A and Hikit B.[864] According to the 2014 DHS Incident Report, the Hikit malware:

> [A]llow[ed] the attackers to create a reverse shell from their C2 [command and control] servers into the infected systems in OPM's network from a remote location anywhere in the world. Wagner reaffirmed the Hikit malware was mostly used for persistence, or maintaining a presence at OPM, though keylogging activity was also observed.[865]

Effectively, the malware was used so that the hackers could "still use it to obtain entry into OPM's network.[866] Hikit in particular has shown to take particular advantage of poor

---

[858] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 19.
[859] ThreatConnect Research Team, OPM Breach Analysis, THREATCONNECT (June 5, 2015), https://www.threatconnect.com/opm-breach-analysis/.
[860] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 10.
[861] Novetta, *Hikit Analysis* at 1 (Nov. 2014), available at: https://www.novetta.com/wp-content/uploads/2014/11/HiKit.pdf
[862] *Id.*
[863] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 27
[864] Saulsbury Tr. at 17.
[865] Wagner Tr. at 17.
[866] Saulsbury Tr. at 18.

internal firewalls and network segmentation.[867] According to one of the earliest analyses of Hikit malware conducted by FireEye, Inc., an attacker was able to tunnel via Remote Desktop and proliferate across the network using previously compromised credentials.[868] This allowed attackers to "create 'hop points' among internal and external network segments" by installing copies of the rootkit in strategic locations to establish new footholds within the target network.[869]

The Hikit malware was well-suited for use on OPM's network. DHS found OPM did not (and may still not) "have tiered network architecture with segmentation between users, databases, applications, and webservers. OPM's network is extremely flat at this time and has little to no segmentation."[870] DHS ultimately recommended: "the server environment should be segmented via firewalls into logically separate internally and externally accessible DMS, web server, application server, and database environment."[871] **The flat network architecture that OPM's legacy environment employed made the agency an ideal target for exploitation by the Hikit malware.**

Malware Discovered during the 2015 Data Breach

Security researchers have suggested a variety of possible threat actors are responsible for the 2015 data breach at OPM.[872] While much of the evidence that would support attribution of the actor to a particular threat actor or actors remains classified, public source documents indicate a group referred to as "Deep Panda" is likely to have been involved based on the attack infrastructure.[873]

Unlike the 2014 data breach, where Hikit malware could be uniquely linked to the Axiom Group, the use of PlugX malware in the 2015 data breach alone is not sufficient to positively identify "Deep Panda" as the culprit. The PlugX employed by the 2015 attackers is commonly used by cyber threat actors and has only become more prevalent since the initial

---

[867] Saulsbury Tr. at 18.
[868] Christopher Glyer & Ryan Kazanciyan, *The "Hikit" Rootkit: Advanced and Persistent Attack Techniques (Part 2)*, FIREEYE (Aug 22, 2012), available at: https://www.fireeye.com/blog/threat-research/2012/08/hikit-rootkit-advanced-persistent-attack-techniques-part-2.html.
[869] *Id.*
[870] June 2014 OPM Incident Report at HOGR0818-001236.
[871] *Id.*
[872] Jeremy Wagstaff, *Hunt for Deep Panda Intensifies in Trenches of U.S.–China Cyberwar*, REUTERS, June 21, 2015, available at: http://www.reuters.com/article/us-cybersecurity-usa-deep-panda-idUSKBN0P102320150621 ("Security researchers have many names for the hacking group that is one of the suspects for the cyberattack on the U.S. government's Office of Personnel Management: PinkPanther, KungFu Kittens, Group 72 and, most famously, Deep Panda. But to Jared Myers and colleagues at cybersecurity company RSA, it is called Shell Crew."); *see also* David Perera, *Agency Didn't Encrypt Feds' Data Hacked by Chinese*, POLITICO (June 4, 2015), available at: http://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655 ("The massive data breach there affected the records of 4.1 million current and former federal employees and may be linked to a Chinese state-backed hacker group known as "Deep Panda," which recently made similarly large-scale attacks on the health insurers Anthem and Premera.").
[873] RSA Incident Response, *Emerging Threat Profile: Shell_Crew* 5 (2014),available at: https://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf.

intrusion in 2014.[874] An analysis of the infrastructure used to hack OPM's network in 2015, however, points toward the likely responsible actor. The adversary's attack infrastructure, which includes the websites used to hack OPM's networks and exfiltrate data, was similar to attack infrastructure used in seemingly unrelated cyber intrusions.

The malicious domains registered for the OPM hack had three distinct characteristics: Marvel comic book superhero names, GMX "throw away" e-mail accounts, and domain names tailored to appear as legitimate portions of OPM's network and training resources.[875] An advanced persistent threat's (APT) attack infrastructure is visible to cybersecurity experts in the form of domain names and their corresponding IP address hosted on C2 servers.[876] How, when, and by whom domain names and IP addresses are created, registered, and used in conducting a cyberattack are therefore important factors in attributing a hack to a particular actor. The adversary that perpetrated the data breach against OPM in 2015 used an attack infrastructure similar to cyberattacks tied to Deep Panda.

Cybersecurity research firms Crowdstrike and ThreatConnect have exposed a number of characteristics of Deep Panda's attack infrastructure.[877] These characteristics were identified during the analysis of several intrusions, including attacks on Wellpoint/Anthem,[878] VAE Inc.,[879] and United Airlines.[880] These attacks bear a striking similarity to the 2015 data breach at OPM.[881] The attacks share several common elements:

- Registrant Names: Domains were registered under names associated with Marvel's Avengers, or actors related to the *Iron Man* franchise and Marvel universe.

---

[874] Chris Brook, *PlugX, Go-to Malware for Targeted Attacks, More Prominent Than Ever*, THREATPOST, (Feb. 10, 2015), available at: https://threatpost.com/plugx-go-to-malware-for-targeted-attacks-more-prominent-than-ever/110936/

[875] ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/.

[876] Wagner testified that one of the reasons he considered the 2015 attackers to be sophisticated was because "[the 2015 attackers] used specifically U.S.-based IP hosting addresses to prevent geolocation rules from being effective." Wagner Tr. at 132.

[877] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/; *see also* Matt Dahl, *I am Ironman: DEEP PANDA Uses Sakula Malware to Target Organizations in Multiple Sectors*, CROWDSTRIKE BLOG (Nov. 24, 2014), available at: http://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/?_ga=1.192876841.2030632883.1465319953.

[878] Drew Harwell & Ellen Nakashima, *China Suspected in Major Hacking of Health Insurer*, WASH. POST, Feb. 5, 2015, available at: https://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html?tid=a_inl.; Elizabeth Weise, *Massive Breach at Health Care Company Anthem Inc.*, USA TODAY, Feb. 5, 2015, available at: http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/.

[879] Ellen Nakashima, *Security Firm Finds Link Between China and Anthem Hack*, WASH. POST, Feb. 27, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack/.

[880] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.

[881] *Id.*

- Registrant Emails: The domains were registered using emails that were a combination of pseudorandom ten-digit alphanumeric usernames and "@gmx[.]com" e-mail accounts.[882]

- Faux Domain Names: Registered domains were tailored to look like legitimate domains hosting resources that belonged to the target organization, or portions of the target's network.[883]

With respect to registrant names, Deep Panda's use of a comic book themed naming convention was previously documented by Crowdstrike during their analysis of a 2014 campaign against, among other targets, the healthcare and government sectors.[884] The agency, using a variety of network monitoring tools, identified three domains as the primary attack infrastructure: opmsecurity.org; wdc-news-post.com; and opm-learning.org.

Malicious Domain	Malicious Registrant	Origional Registrant Email	Associated Incident
opm-learning[.]org	tony stark	vrzunyjkmf@gmx[.]com	OPM Breach
opmsecurity[.]org	Steve Rogers	tAPRhpALhl@gmx[.]com	OPM Breach
wiki-vaeit[.]com	Tony Stark	EwibAFNxEe@gmx[.]com	VAE, Inc. Targeting Campaign
sharepoint-vaeit[.]com	Natasha Romanoff	yXDlqMRNdM@gmx[.]com	VAE, Inc. Targeting Campaign
ssl-vaeit[.]com	Dubai Tycoon	aArwcsyHFb@gmx[.]com	VAE, Inc. Targeting Campaign
ssl-vait[.]com	John Nelson	aArwcsyHFb@gmx[.]com	VAE, Inc. Targeting Campaign
marsale[.]net	Mark Wahlberg	eumyjxkywn@gmx[.]com	Unidentified
united-airlines[.]net	James Rhodes	enijswwxsk@gmx[.]com	Unidentified

ThreatConnect chart shows similar registrant names, e-mails, and domains—evidence of a larger, more complex campaign[885]

Deep Panda registered their attack infrastructure using the names of Marvel's Avengers characters and other names associated with the film franchise:

- Tony Stark (a.k.a. Iron Man).

- Steve Rogers (a.k.a. Captain America).

- Natasha Romanoff (a.k.a. Black Widow).

- James Rhodes (a.k.a. War Machine).

- John Nelson (the visual effects supervisor for the Marvel film *Iron Man*).[886]

---

[882] *OPM Breach Analysis: Update*, THREATCONNECT (last visited June 15, 2016), https://www.threatconnect.com/opm-breach-analysis-update/.
[883] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.
[884] Matt Dahl, *I am Ironman: DEEP PANDA Uses Sakula Malware to Target Organizations in Multiple Sectors*, CROWDSTRIKE BLOG (Nov. 24, 2014), available at: http://www.crowdstrike.com/blog/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/?_ga=1.192876841.2030632883.1465319953.
[885] ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/.
[886] *John Nelson Biography*, IMDB, available at: http://www.imdb.com/name/nm0625471/?ref_=fn_al_nm_1.

- Dubai Tycoon (the name of an uncredited role in the Marvel film *Iron Man* portrayed by noted rapper and Wu-Tang Clan member Ghostface Killah).[887]

With respect to registrant email addresses and domain names, the original registrant's email was always a random alphanumeric with a @gmx.com email address, and the domains had OPM themed names.

On April 25, 2014, actors registered the malicious domain "opmsecurity.org," under the name "Steve Rogers" using the e-mail address "tAPRhpALhl@gmx.com."[888] Shortly after the "Big Bang" concluded and just eighteen days after the *New York Times* broke news of the breach on July 9, 2014,[889] another OPM-themed C2 node was established by the same actors. On July 29, 2014, the attackers registered the OPM-themed domain "opm-learning[.]org." The domain was registered by "Tony Stark" using the e-mail address "vrzunyjkmf@gmx[.]com."[890]

In addition, Deep Panda's attack infrastructure typically involves domain names tailored to look like legitimate domains that belong to the target organization.[891] For instance, the security firm ThreatConnect has tied the use of "Wellpoint look-alike domains to a series of targeted attacks launched in May 2014 that appeared designed to trick Wellpoint employees into downloading malicious software tied to the Deep Panda hacking gang."[892]

Domains such as we1lpoint.com or myhr.we1lpoint.com were used in the course of a campaign against Anthem.[893] Security expert Brian Krebs stated: "[It] appeared that whoever registered the domain was attempting to make it look like 'Wellpoint,' the former name of Anthem before the company changed its corporate name in late 2014."[894] These victim-centric domains could easily fool network monitors as they, at first glance, appear legitimate, but under further analysis are proven to be malicious.

---

[887] *Iron Man Trivia*, IMDB, http://www.imdb.com/title/tt0371746/trivia (last visited June 30, 2016). ("Ghostface Killah, a long-time fan of the Iron Man comics (he uses the aliases 'Ironman' and 'Tony Starks,' titled his 1996 album 'Ironman' and sample clips of Iron Man (1966)), had a cameo as a Dubai tycoon. However, his scene was cut from the final film. Jon Favreau apologized to Ghostface and used his "We Celebrate" video in the film.").

[888] *OPM Breach Analysis: Update*, THREATCONNECT (last visited June 15, 2016), available at: https://www.threatconnect.com/opm-breach-analysis-update/.

[889] Michael S. Schmidt, David E. Sanger & Nicole Perlroth, *Chinese Hackers Pursue Key Data on U.S. Workers*, N.Y. TIMES, July 9, 2014, http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?_r=0.

[890] *OPM Breach Analysis: Update*, THREATCONNECT, available at: https://www.threatconnect.com/opm-breach-analysis-update/.

[891] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.

[892] Brian Krebs, *Premera Blue Cross Breach Exposes Financial, Medical Records*, KREBS ON SECURITY (Mar. 17, 2015, 5:42 PM), available at: http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/#more-30380.

[893] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.

[894] Brian Krebs, *Anthem Breach May Have Started in April 2014*, KREBS ON SECURITY (Feb. 15, 2015, 10:34 AM), available at: http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/.

Deep Panda also appeared to name the domains to emulate portions of the target's network or to mimic organizationally-related resources hosted outside the target's network.[895] In the case of VAE, Deep Panda made the domains look like company-related Sharepoint or Wiki resources by naming them "sharepoint-vaeit.com" and "wiki-vaeit.com."[896] In the 2015 OPM breach, the malicious domains used for command and control, "opm-learning[.]org" and "opmsecurity.org," resemble the websites OPM uses for its annual information technology security awareness training, "opmsecurity.golearning.org" and "security.golearnportal.org."[897] This training is required for all full-time and part-time federal employees and contractors who have access to OPM's networks.[898]

The faux-domain naming used in these hacks is a Deep Panda "calling card," but it also reveals information about Deep Panda's TTPs. These victim-centric domains could slip past network monitors as they, at first glance, appear legitimate. The domains are designed to fool employees into thinking they are legitimate. After clicking on a link sent through a spear phishing e-mail, attackers can download malware into the company's network by exploiting vulnerabilities in the victim's web browser. This technique, called a "watering hole attack,"[899] is a strategy that uses hacked websites or fake, legitimate-looking domains to download malware into a victim's computer.[900] Watering hole attacks are a technique heavily favored by, though not exclusive to, the Deep Panda threat actor group.[901]

Another common element of Deep Panda's campaigns is it often relies on some of the same attack infrastructure for multiple intrusions, including the breach into OPM's network.[902] The following domains were active on OPM's systems during the course of incident response:[903]

Entry #	IP	Domain
Entry 1	[redacted]	Wiki-vaeit.com Sharepoint-vae.com ssl-vaeit.com Wiki-vaeit.com
Entry 2	[redacted]	We1lpoint.com

[895] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.
[896] *Id.*
[897] *OPM Breach Analysis: Update*, THREATCONNECT (last visited June 15, 2016), available at: https://www.threatconnect.com/opm-breach-analysis-update/.
[898] Saulsbury Tr. at 34.
[899] So named because it resembles a strategy employed by predators, who will lie in wait to ambush prey at a site they are known or expected to frequent like a watering hole.
[900] Will Gragido, *Lions at the Watering Hole – The "VOHO" Affair*, RSA, (Jul 20, 2012), https://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/
[901] Adam Greenberg, *Watering Hole Attacks are Becoming Increasingly Popular, Says Study*, SC MAGAZINE, Sept. 27, 2013, available at: http://www.scmagazine.com/watering-hole-attacks-are-becoming-increasingly-popular-says-study/article/313800/ (quoting Nick Levay, chief security officer with Bit9, "Watering holes have been on the rise in the past few years and a lot of hackers that were using spear phishing attacks to target people have started using watering holes,' said Levay, explaining that while watering holes typically target a specific group or community, he has seen narrower variants that, for example, will only target a certain range of IP addresses.")
[902] *See e.g.* ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/.
[903] OPM Domain Name Log (Unredacted) at HOGR0724-D00893-95-UR (OPM Production: Dec. 22, 2015).

		Extcitrix.wel1point.com Myhr.wel1point.com Hrsolultions.wel1point.com
Entry 3	[redacted]	drongobast.com efuelia.com gandaband.com kopirabus.com macroxaz.com mustufacka.com ns1.figaina5.com ns8.figaina5.net nsa.figaina5.net
Entry 4	[redacted]	nsa.org.cn
Entry 5	[redacted]	cdn.servehttp.com smtp.outlookssl.com

Entries 1 and 2 in the above chart are malicious domains also used by Deep Panda against VAE and Wellpoint/Anthem systems.[904] Seven of these domains (Wiki-vaeit.com, Sharepoint-vae.com, ssl-vaeit.com, We11point.com, Extcitrix.wel1point.com, Myhr.wel1point.com, Hrsolultions.wel1point.com) were active on OPM's systems during the 2015 data breach and share common identifiers with the primary infrastructure used to perpetrate the breach against OPM discovered in 2015, including Avengers-themed names and GMX email addresses. Threat researchers tied attacks at VAE and Anthem to a "group known by a number of names, including Deep Panda, Axiom, Group 72, and the Shell_Crew."[905]

Testimony shows OPM security personnel also connected the 2015 attack to Deep Panda. Saulsbury testified:

> Q. So my question is as a result of the April 2015 cyber intrusion, was OPM SOC able to draw any conclusions as to whom or what organization might have been responsible for the malicious activity? And again, to the extent you can answer without revealing any classified information.
>
> A. Right, so to clarify, I do not have a clearance. I do not have access to any classified information. The only unclassified information that we have was that some of those Marvel character-related domain names or domain registrants, they showed up in a -- I believe it was a Mandiant report, incident response report regarding a publicized data breach for a healthcare provider, but I can't recall specifically which it was at this time. But the Mandiants dubbed the attacker Deep Panda, (emphasis added) so

[904] Threat Connect Research Team, *The Anthem Hack: All Roads Lead to China*, THREATCONNECT (Feb. 27, 2015), available at: https://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.
[905] Brian Krebs, *Anthem Breach May Have Started in April 2014*, KREBS ON SECURITY (Feb. 15, 2015, 10:34 AM), available at: http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/.

> based on that domain registrant correlation, that is the only indication, or at least on the unclassified side, that we have that that may be the same attacker.[906]

Saulsbury's testimony was corroborated by Coulter, who testified about the Plug X malware and other evidence Cylance found on OPM's systems. Coulter stated:

> A. So I'll use the word 'actor,' the ones that were identified in prior exhibits. You had Shell Crew, or sometimes known as Deep Panda, as well as Deputy Dog, and it has many, many other names. So those were the two that, at least as it relates to the industry research being done, that the malware that we found was closest related to it. By no means are we saying it was them; it's just it was a relationship or similarity.
>
> Q. Okay. Are those two generally associated with a particular country?
>
> A. In the industry, yes.
>
> Q. Can I ask which country?
>
> A. [redacted][907]

The 2015 OPM attackers' use of malicious domains similar to, or even the same as, those used in attacks against VAE and Wellpoint (Anthem) show Deep Panda likely perpetrated the data breach against OPM that was discovered in 2015. The similarities in the pseudorandom 10-digit GMX address, OPM-themed domains, and Avengers-themed registrants are evidence that the infrastructure was created and utilized by the same group. Documents and testimony connect Deep Panda and Axiom, and therefore the 2014 and 2015 data breaches at OPM were likely connected, and possibly coordinated.

2014 & 2015: Likely Connected, Possibly Coordinated

While OPM has maintained the cyberattacks conducted against their systems in 2014 and 2015 were separate occurrences, documents and testimony show a broader campaign against the information of federal workers by state-sponsored hacking organizations (Deep Panda and Axiom) were responsible.

Under a theory advanced by threat researcher FireEye, "many seemingly unrelated cyber-attacks may, in fact, be part of a broader offensive fueled by a shared development and logistics

[906] Saulsbury Tr. at 83.
[907] Coulter Tr. at 93.

infrastructure – a finding that suggests some targets are facing a more organized menace than they realize."[908]

The overlapping use of malware and exploits, or as FireEye called it, a "shared malware-builder tool,"[909] by Axiom and Deep Panda show the data breaches at OPM in 2014 and 2015 were likely connected, possibly coordinated.

If FireEye's theory is true, either Axiom and Deep Panda's efforts to collect data from OPM's systems in 2014 and 2015 were connected via a common supplier of cyber resources, or that Axiom and Deep Panda's efforts were actively coordinated by that supplier. While FireEye terms this common-supplier a "digital quartermaster," other threat researchers have identified a similar shared resources model. A researcher at PricewaterhouseCoopers LLP stated:

> In our experience, very few attackers have the patience to maintain completely distinct infrastructure with multiple registrars, name servers and hosting providers at the same time . . . in our view, the hypothesis with the highest probability is that groups of attackers share resources leading to overlaps – this appears to be an ever more common feature – with malware families, builders, and even sometimes hosting infrastructure being shared between disparate actors with a common goal.[910]

Documents show Axiom used Hikit malware to attack OPM's network in 2014 and were targeting the background investigation data stored on the PIPS system that was eventually stolen by Deep Panda using PlugX malware. Documents show Axiom and Deep Panda had more in common than their target.

Both have been tied to the use of Plug X and Hikit malware.[911] Among the challenges in making this assertion are the naming conventions used by the threat researcher community in analyzing data breaches and persistent threat actors. For example, threat researchers at Cisco stated that "hikit, according to our data [is] unique to Group 72 and to two other threat actor groups." Group 72 is an alias associated with a state-sponsored "espionage" group known by a number of names, including Deep Panda."[912] But Hikit is not the only malware that Axiom and

---

[908] FireEye, *Supply Chain Analysis: From Quartermaster to SunshopFireEye* at 3, available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-malware-supply-chain.pdf.
[909] *Id.*
[910] Chris Doman & Tom Lancaster, *ScanBox Framework – Who's Affected, and Who's Using It?*, PWC (Oct. 27, 2014), available at: http://pwc.blogs.com/cyber_security_updates/2014/10/scanbox-framework-whos-affected-and-whos-using-it-1.html.
[911] FireEye, *Supply Chain Analysis: From Quartermaster to SunshopFireEye* at 3, available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-malware-supply-chain.pdf
[912] Brian Krebs, *Anthem Breach May Have Started in April 2014*, KREBS ON SECURITY (Feb. 15, 2015, 10:34 AM), available at: http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/ (It is noteworthy that Brian Krebs links Deep Panda and Axiom); *see also* Andrea Allievi et al, Cisco, *Deconstructing and Defending Against Group 72*, (2014), available at: http://www.talosintel.com/files/publications_and_presentations/papers/Cisco_security_Group72_wp.pdf.

Deep Panda use:[913]

Malware Name	Deep Panda	Axiom
Gh0st Rat (Moudour, Mydoor)	X	X
Poison Ivy (Darkmoon, Breut)	X	X
HydraQ (9002RAT, McRAT, Naid, Roarur, Mdmbot)	X	X
ZxShell (Sensode)	X	X
Deputy Dog (Fexel)	X	X
Derusbi	X	X
PlugX (Thoper, Sogu, Korplug, Kaba, DestroyRAT)	X	X
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
Sakula (Sakura, Sakurel)	X	
Mivast RAT	X	
Hurix	X	

In addition to an overlapping repertoire of malware, Axiom and Deep Panda have both been linked to the use of the "Elderwood Framework."[914] Symantec Security Response identified attackers employing "re-use components of an infrastructure" which they named the "Elderwood Framework," after "a source code variable used by the attackers."[915] The Elderwood Framework is effectively a library of exploits that hackers can use to conduct malicious operations.[916] Novetta cited Axiom's use of similar TTPs, tools, and other attack infrastructure, including "Elderwood platform attacks," in 2011, 2012, and 2014.[917] According to Symantec, "Black Vine," a.k.a. Deep Panda, also used the Elderwood Framework.[918]

The overlapping TTPs, malware, and attack infrastructure that Axiom and Deep Panda use suggests these groups share a "digital quartermaster," a central supplier of malicious tools, tactics, and techniques to a variety of state-sponsored espionage groups. This explains why the same group of hackers has launched attacks under several different names—Axiom, Deep Panda, Shell_Crew, Deputy Dog, etc.

With respect to the OPM breach, the attack infrastructure and common malware indicates Axiom and Deep Panda are probably connected. The overlapping timeframe of the attacks on OPM also suggest that a connection between the perpetrators.

---

[913] *See*, Novetta, *Operation SMN: Axiom Threat Actor Group Report*, at 4; *see also*, ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), https://www.threatconnect.com/opm-breach-analysis/. *See also,* Brian Krebs, *Anthem Breach May Have Started in April 2014*, KREBS ON SECURITY (Feb. 15, 2015, 10:34 AM), http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/. *See also,* Liam Tung, *Anthem Health Insurance Hackers are a Well-Funded, Busy Outfit*, CSO, July 29, 2015, http://www.cso.com.au/article/580685/anthem-health-insurance-hackers-well-funded-busy-outfit/.

[914] Gavin O'Gorman & Geoff McDonald, Symantec, *The Elderwood Project* (last visited June 15, 2016), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf.

[915] *Id.*

[916] *Id.*

[917] Novetta, *Operation SMN: Axiom Threat Actor Group Report* at 12.

[918] Liam Tung, *Anthem Health Insurance Hackers are a Well-Funded, Busy Outfit*, CSO, July 29, 2015, available at: http://www.cso.com.au/article/580685/anthem-health-insurance-hackers-well-funded-busy-outfit/.

Documents show that while OPM was monitoring the 2014 attacker's movements in May 2014, the 2015 attackers were able to drop PlugX malware onto servers connected to the background databases the 2014 attackers were targeting.[919] Within forty-five days of their initial entry into OPM's networks, the 2015 attackers were able to gain access to the personnel records and background investigation databases, establish a "late-stage" attack infrastructure, and begin data exfiltration.

The speed at which the 2015 attackers were able to escalate access from initial entry to end-stage presence and exfiltration suggests a level of familiarity with OPM's environment. This creates the appearance that the 2015 attackers relied on information obtained by the 2014 hackers, who had access to OPM's network for years and were unable to compromise the most sophisticated systems, such as those holding background investigation data.

According to Saulsbury, the documents the 2014 attacker exfiltrated from OPM provided an attacker - or any associated group with (directly or indirectly) - an advantage.[920] As Mr. Saulsbury explained the documents provide "more familiarity with how the systems are architected. Potentially some of these documents may contain accounts, account names, or machine names, or IP addresses, which are relevant to these critical systems."[921]

The documents the 2014 attackers stole may be characterized as documents that provide overviews of key systems (such as PIPS, EPIC/eQIP, and Fingerprint Transactional System) and provide information as to who has access to those systems.[922] The documents effectively provide a roadmap to how the background and personnel data is ingested into OPM's systems, how OPM integrates those systems with the government contractors working on them, and who has access to those systems. It is the kind of information that would accelerate an attacker's familiarity with OPM's most highly sensitive information and could explain the speed with which the 2015 attacker was able to establish access, orient themselves, escalate network authorities, and penetrate the most highly sensitive data repositories on OPM's network.

Documents obtained by the Committee show additional evidence of a connection between the 2014 attacker and the 2015 attack. For example, the 2015 attacker persisted in their intrusion even after the public announcement of the 2014 data breach on July 9, 2014, and continued exfiltrating OPM's background investigation data. This shows the 2015 attackers had sufficient awareness of OPM's security protocols and were not worried despite the heightened state of security that was put in place. This suggests a degree of collusion or shared tasking between the two attackers, enough so that the 2015 attacker would be comfortable that earlier efforts would pave the way and the subsequent mitigation steps taken by OPM would not disrupt the 2015 attackers' ongoing operation.

Regardless of the names of the threat actor groups that were conducting malicious activity on OPM's systems it should have been clear to OPM in the wake of the 2014 data breach

[919] June 9, 2015 DMAR at HOGR0724-001154.
[919] June 2014 OPM Incident Report at HOGR0818 -001245.
[921] Saulsbury Tr. at 27-28.
[922] June 2014 OPM Incident Report at HOGR0818 -001245.

that they were facing a sophisticated, well-resourced adversary with connections to a spectrum of state-sponsored threat actors. Private sector threat researchers were connecting the dots between the targeted campaign against federal employees, as evidenced by the data breaches at Anthem, Premera, USIS, KeyPoint, and should have heightened awareness of federal agencies like OPM holding large sensitive data repositories.

Chapter 7: OPM's OCIO and its Federal Watchdog

Pursuant to the Inspector General (IG) Act of 1978, Inspectors General "provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies relating to the administration of such programs and operations and the necessity for and progress of corrective action."[923] When President Carter signed the IG Act of 1978, he charged the IGs to always remember that their ultimate responsibility is not to any individual but to the public interest.[924]

The relationship between OPM's Office of the Inspector General (OIG) and its OCIO became strained while Katherine Archuleta served as Director and Donna Seymour as CIO. In fact, the relationship deteriorated to the point that IG Patrick McFarland took the drastic step of issuing a memorandum to Acting Director Beth Cobert to share "serious concerns" regarding the OCIO on July 22, 2015.[925]

The memorandum was issued just 12 days after Cobert was appointed Acting Director of the agency. During her nomination hearing before a Senate Committee,[926] Cobert was emphatic that she takes the relationship with the IG seriously, especially as it relates to enhancing cybersecurity.[927] Cobert met with the IG on her first day at OPM,[928] and she instituted regular meetings with the OIG thereafter.[929]

Despite serious concerns raised by the IG and Congress about Seymour's fitness to serve as CIO in the summer of 2015,[930] Cobert maintained support for Seymour and allowed her to remain on the job until her retirement on February 22, 2016.[931] The Committee obtained testimony in October 2015 that shows problems between the OCIO and the OIG persisted through the fall of 2015. An OIG employee testified that the relationship was strained, and the onus was on OIG staff to "chase down" information from the OCIO.[932]

---

[923] Inspector General Act of 1978 § 2; 5 U.S.C. app. § 2 (2012) (as amended).
[924] Council of the Inspectors Gen. on Integrity and Efficiency, *IG Act History* available: https://www.ignet.gov/content/ig-act-history.
[925] OIG Memo, *Serious Concerns*.
[926] *Nomination of the Honorable Beth F. Cobert to be Director, Office of Personnel Management: Hearing Before the S. Comm. on Homeland Sec. & Gov't. Affairs*, 114th Cong. (2016).
[927] *Id.*
[928] *Id.*
[929] *Incorporating Social Media into Federal Background Investigations: Hearing Before the Subcomm. on Gov't Operations and Subcomm. on Nat'l Sec.* of the *H. Comm. Oversight & Gov't Reform* 114th Cong. at 1:12.35 (2016).
[930] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Interim Dir., U.S. Office of Pers. Mgmt (Aug. 6, 2015); *see also* Letter from 18 Members of Congress, to Barack Obama, President, United States (June 26, 2015) (raising concerns about OPM Director Katherine Archuleta and OPM Chief Information Officer Donna Seymour).
[931] Aaron Boyd, *OPM CIO Seymour Resigns Days Before Oversight Hearing*, FEDERAL TIMES (Feb. 22, 2016) available at: http://www.federaltimes.com/story/government/it/cio/2016/02/22/opm-cio-seymour-resigns/80766440/; Billy Mitchell, *Office of Personnel Management CIO Donna Seymour Retires*, FEDSCOOP, (Feb. 22, 2016) available at: http://fedscoop.com/opm-cio-seymour-retires; Ian Smith, *OPM CIO Donna Seymour Resigns*, FEDSMITH (Feb. 22, 2016) available at: http://www.fedsmith.com/2016/02/22/opm-cio-donna-seymour-resigns/.
[932] Special Agent Tr. at 46, 65-66.

Overall, however, the OCIO's relationship with the OIG steadily improved under Acting Director Cobert's leadership, and as of this report's publication, both offices report it to be without conflict.[933]

The IG's Memorandum of Concern

On July 22, 2015, the OPM IG wrote Acting Director Cobert to call attention to four situations where he felt the OCIO hindered his office's efforts, and five instances where he contended the OCIO provided incorrect and/or misleading information.[934]

MEMORANDUM FOR BETH F. COBERT
Acting Director

FROM: PATRICK E. McFARLAND
Inspector General

SUBJECT: Serious Concerns Regarding the Office of the Chief Information Officer

The memorandum stated:

> In certain situations, the OCIO's actions have hindered the OIG's ability to fulfill our responsibilities under the Inspector General Act of 1978, as amended (IG Act). Further, we have found that the OCIO has provided my office with inaccurate or misleading information, some of which was subsequently repeated by former OPM Director Katherine Archuleta at Congressional hearings.[935]

McFarland pointed out that the breakdown in the relationship stood in stark contrast to the relationship the OIG had with the OCIO in the past.[936] McFarland served as the agency's watchdog for twenty-six years.[937] Documents show the relationship between the OIG and OCIO did in fact deteriorate after being strong for years.

---

[933] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.) (hearing cancelled); *see also Incorporating Social Media into Federal Background Investigations: Hearing Before Subcomm. on Gov't Operations and Subcomm. on Nat'l Sec. of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. at 1:12.35 (2016).

[934] U.S. Office of Pers. Mgmt. Office of Inspector Gen., Memorandum from Inspector Gen. Patrick McFarland to Acting Dir. Beth Cobert, Serious Concerns Regarding the Office of the Chief Information Officer (July 22, 2015) [hereinafter OIG Serious Concerns Regarding OCIO (July 22, 2015).]

[935] *Id.* at 1.

[936] *Id.*

[937] Carten Cordell, *OPM Inspector General Resigns, Leaving in February*, FED. TIMES, Feb. 3, 2016, http://www.federaltimes.com/story/government/management/agency/2016/02/03/opm-inspector-general-resigns-leaving-february/79756822/.

For example, in the April 2008 Semi-Annual Report to Congress, McFarland reported that then-Director Linda M. Springer had initiated a series of actions "to make sure that all OPM employees clearly understood what PII meant, the importance of protecting PII, and their responsibilities in protecting it."[938] The IG was to play an integral role in the efforts. The report stated:

> Director Springer requested that the OIG conduct an audit of one of OPM's largest program offices to ensure that they had developed and implemented effective controls over PII. . . . PII has also become a routine topic of discussion at the Agency's Information Technology Security Working Group meetings. The group was set up by the Chief Information Officer to ensure that information technology (IT) security and privacy policies, procedures and directives are communicated to all OPM program offices. On the technical side, OPM has made significant progress in implementing OMB requirements to safeguard PII.[939]

Former Inspector General Patrick McFarland testifies about data breaches

In 2015, however, McFarland had to resort to a public notification to Acting Director Cobert to call attention to the fact that his office was being undermined. McFarland wrote:

> In the past, the OIG has had a positive relationship with the OCIO. Although the OIG may have identified problems within the OCIO's areas of responsibility, we all recognized that we were on the same team, and the OCIO would leverage our findings in an effort to bring much needed attention and resources to OPM's information technology (IT) program.

---

[938] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2007 to March 31, 2008* (Mar. 2008), https://www.opm.gov/news/reports-publications/semi-annual-reports/sar38.pdf.
[939] *Id.*

> Unfortunately, this is no longer the case, and indeed, recent events make the OIG question whether the OCIO is acting in good faith.[940]

McFarland's memorandum was released to Congress and the public.[941] Chairman Chaffetz shared the IG's concerns. In a letter to Cobert, Chairman Chaffetz stated that he lost confidence in Seymour in the wake of the agency's announcement of the breaches, that his concerns were "amplified" by the IG's memorandum, and keeping Seymour in place only added "insult to injury" to those whose personal and sensitive information was stolen in the breaches.[942]

> On June 26, I communicated to President Obama that I have lost confidence in Ms. Seymour's ability to execute her role as CIO. Despite repeated warnings from the OPM Inspector General, Ms. Seymour failed to prevent breaches of personally-identifiable information, harming over 22 million federal employees and other individuals, and weakening our national security. As a result, I asked the President to address this serious issue by removing Ms. Seymour from her position.
>
> I am deeply troubled Ms. Seymour remains at her post over a month after this request was made. My concerns about Ms. Seymour's ability to serve are amplified by a communication the Committee received from the Inspector General. In a letter dated August 3, 2015, OPM's IG notified me that on July 22, 2015 a memorandum was sent to you, and the letter advised me that "there have been situations where actions by the OCIO have interfered with, and thus hindered, the OIG's work. Further, the OCIO has repeatedly provided the OIG with inaccurate or misleading information."[1]

Excerpt from August 6, 2015 letter from Chairman Chaffetz to Acting Director Cobert

Cobert did not remove Seymour. In fact, Cobert gave Seymour a vote of confidence. *FedNewsRadio* reported:

> An OPM spokesman said by email that Cobert is pleased with Seymour and the entire CIO team's efforts to improve OPM's cybersecurity. . . . The [OPM] spokesman said Cobert responded to the IG's letter, saying 'In her first four weeks at OPM she has observed that the team, including the Office of the Chief Information Officer — working side-by-side with experts from across the federal government — has been working incredibly hard to enhance the security of our information technology systems and support those who have been affected by the recent cybersecurity incidents. The recent results of the Cybersecurity Sprint demonstrate the progress that has been made, although everyone recognizes there is more to do.'[943]

---

[940] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 1.
[941] *Id.*
[942] Letter from the Hon. Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform, to the Hon. Beth Cobert, Interim Dir., U.S. Office of Pers. Mgmt (Aug. 6, 2015).
[943] Jason Miller, *IG, Chaffetz Increase Heat on OPM CIO,* FEDNEWSRADIO, Aug. 6, 2015, available at: http://federalnewsradio.com/opm-cyber-breach/2015/08/ig-chaffetz-increase-heat-opm-cio/. The Cybersecurity Sprint was meant to increase the security of agencies systems. For additional information, *see* Exec. Office of the

Cobert said she was "committed to ensuring a cooperative relationship" between her teams and the OIG.[944] Cobert added that she "discussed the importance of the issue" with her leadership team and said they "are fully supportive of rebuilding a productive relationship, and fully understand how that will help us collectively deliver on OPM's mission."[945] The extremely serious nature of the concerns, however, raise questions about the decision to stand by Seymour.

Four Instances Where the OCIO Failed to Cooperate Fully

McFarland's letter to Cobert on July 22, 2015 identified four situations where the OCIO failed to cooperate with his office to the detriment of the agency.

Seymour failed to appropriately notify the IG of the April 2015 intrusion detection

In April 2015, the agency identified an unknown Secure Sockets Layer (SSL) certificate beaconing to a site (opmsecurity.org) that was not associated with OPM.[946] The agency reported this finding to US-CERT on April 15, 2015.[947] On Friday, April 17, 2015 at 11:39 a.m., OPM submitted several more questionable files to US-CERT,[948] and by 5:19 p.m. that evening, US-CERT confirmed the malicious nature of the executable files that OPM reported.[949]

The IG was not notified by OCIO—or anyone else at OPM—until one week later, on April 22, 2015.[950]

Under OPM's "Incident and Response and Reporting Guide," the OIG is an integral part of incident response.[951] For example, the Guide states that the OIG must be notified immediately if criminal activity is suspected.[952] The Guide instructs key OPM personnel to be trained in how to make notifications in a manner that serves the best interests of forensic investigations. It states that the OPM Computer Incident Readiness Team (OPM-CIRT) "must be trained in such areas as whom to contact when an incident occurs, how to preserve forensic evidence, and how

---

President, Press Release, *FACT SHEET: Enhancing and Strengthening the Federal Government's Cybersecurity* (June 12, 2015) https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/enhancing-strengthening-federal-government-cybersecurity.pdf.

[944] Memorandum from the Hon. Beth Cobert, Acting Dir., U.S. Office of Pers. Mgmt. to Patrick McFarland, Inspector Gen., U.S. Office of Pers. Mgmt., *Your Memo of July 22, 2015* (Aug. 3, 2015) [hereinafter Cobert Response to OIG Serious Concerns Regarding OCIO].

[945] *Id.*

[946] AAR Timeline – Unknown SSL Certificate (April 15, 2015) at HOGR020316-001922-1923 (OPM Production: April 29, 2016).

[947] *Id*; Email from [redacted] to CIRT (OPM) (April 15, 2015, 6:54 p.m.) at HOGR0724-000868 (OPM Production: Dec. 22, 2015).

[948] Email from [redacted] to Brendan Saulsbury, Senior Cyber Security Engineer, SRA (Apr. 17, 2015, 5:19 p.m.) at HOGR0724-000872- 75 (OPM Production: Dec. 22, 2015).

[949] *Id.*

[950] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 3.

[951] U.S. Office of Pers. Mgmt., *Incident Response and Reporting Guide* at 3 (July 2009).

[952] *Id.* The Special Agent testified in October 2015 that this Guide was still the most current despite being dated July 2009. *See* Special Agent Tr. at 8.

to eradicate the various types of incidents. The training must also include when incidents are reported to US-CERT, the OPM IG, and appropriate law enforcement agencies."[953] The Guide states that "[c]omputer incidents are generally a lot easier to handle when reported promptly" and requires the Network Management Group Chief to help notify in a "timely manner" all "responsible parties," including the Assistant Inspector General for Investigations in the OIG.[954]

Documents and testimony show the OCIO failed to notify the OIG in a timely manner in April 2015. In fact, the IG found out about the breach by coincidence. The OIG Special Agent in Charge (SAC) ran into OCIO Director of IT Security Operations Jeff Wagner in the hallway. Wagner asked the SAC to meet later in the day (at which time the SAC was informed of the first breach)."[955]

The SAC, noticed Wagner on the sixth floor of OPM around lunch time, which was unusual because Wagner worked on a different floor. The SAC testified:

> As I recall it, it was truly a chance encounter. I was exiting from the elevator on the sixth floor. I was walking down the hallway. Jeff Wagner and a coworker -- I don't recall who the coworker was or to this day don't remember -- was walking into the Federal Investigative Service Office, which is in the hallway of the sixth floor, and as I was approaching Jeff, waved, nodded, as I know who Jeff is. And Jeff said: Hey, when [you] get a chance, come down to my office. And we -- or I continued on into my office.[956]

The SAC testified that the entire conversation lasted no longer than thirty seconds, and that "I would describe this as a conversation in passing. Literally, he was walking into an office; I was walking towards my office."[957]

The SAC testified to not knowing what Wagner wanted to discuss at the meeting Wagner requested.[958] In fact, the SAC thought Wagner may have wanted to discuss Federal Employee Health Benefits (FEHB) program carriers. The SAC stated:

> So I immediately went back to my office, and as I recall, I thought this was in reference to another potential breach. We had the Anthem breach earlier, I believe February 2015. March of 2015, you had the Premera. Those were large FEHBP carriers. We were still trying to sort out what the impact to not only FEHBP subscribers but the FEHBP as a whole and its financial integrity. I immediately thought this was another breach of a FEHBP carrier when I left Jeff.[959]

---

[953] U.S. Office of Pers. Mgmt., *Incident Response and Reporting Guide* at 12.
[954] *Id.*
[955] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 3.
[956] Special Agent Tr. at 11.
[957] *Id* at 12.
[958] *Id.*
[959] *Id.* at 12-13.

When the SAC visited Wagner later that afternoon, the SAC learned OPM had suffered an intrusion. Wagner handed the SAC a security incident timeline that included a series of dates and bullets.[960] The earliest date was April 15, 2015, and there was an attached description that stated: "Zero day, malicious activity found."[961] The SAC testified: "what immediately jumped out to me was internal notifications were made. The FBI was called. Also the United States Department of Homeland Security, US-CERT team, the Computer Emergency Response Team, had been called and notified."[962]

The SAC recalled being "shocked" that law enforcement was in the building and that the OIG was unaware.[963] With respect to why it was important for the OIG to receive timely notice, the SAC stated:

> A. There are several reasons why. First, the IG Act. It's the agency's responsibility to notify the IG of potential incidents or situations that impact the agency so the IG can timely -- or do its job in a timely matter of notifying Congress.
>
> You have the FISMA Act, which is the Federal Information Management Security Act, which requires notification of the appropriate IG, of what I recall of a potential -- or what I recall and believe it states of a potential situation -- we would be the appropriate IG in that situation -- and by their own incident and reporting guide of 2009.
>
> The other thing is just basically common courtesy. I would expect Jeff's office -- especially if you have people walking into the building with guns. I'm also responsible if there is an active shooter in the building of deploying assets, and it can obviously be a very terrible situation if we don't realize what other people are in the building that are armed at that particular time.
>
> Q. So you're saying if other law enforcement officers were in the building --
>
> A. Sure.
>
> Q. you would be the one responsible for coordinating with those individuals?
>
> A. Correct.[964]

---

[960] *Id.* at 13-14
[961] *Id.*
[962] *Id.* at 14.
[963] *Id.* at 16.
[964] *Id.* at 15-16.

The SAC testified that Wagner said OPM had no intention of notifying the public, and that the OIG disagreed with that plan.[965] The SAC testified that Wagner said "there was no need" to notify the public, and that Wagner believed there was "no evidence" the agency had lost information to the attackers, and that the situation was being carefully monitored.[966] **By April 22, 2015, however, OPM already found evidence of a serious breach**. OPM eventually announced that it lost the personnel records of 4.2 million federal employees on June 4, 2015.[967]

The failure of the OCIO to notify the IG in a timely manner undermines the important role Congress has established for the IGs. Like all federal watchdogs, McFarland's ultimate responsibility during this time was not to any individual, but to the public interest.[968] Being prevented from taking part in the investigation into the cyber intrusion from day one hampered the IG's ability to effectively carry out its work on behalf of the public, and also undermined the public's trust that the agency was acting in good faith. As conveyed by McFarland, "Failure to include OIG investigators and auditors from the beginning of the incident impeded our ability to coordinate with other law enforcement organizations and conduct audit oversight activity."[969]

Seymour failed to notify the OIG of the loss of background investigation data in a timely manner

With respect to the loss of background investigation materials, the Special Agent testified that the OIG was notified unintentionally. The SAC testified:

> So, it was another right place at the right time type of situation. On or about May 18, 2015, I had received information that there was another breach at an FEHBP carrier, this time being CareFirst. CareFirst is an extremely large FEHBP carrier, and this caused us great concern. I called Jeff [Wagner] on or about May 18th, May 19th, that evening, asking if he had heard anything about the CareFirst situation.[970]

The SAC stated that Wagner had not heard anything about CareFirst, and they agreed to continue checking-in with each other.[971] Two days later, on May 20, 2015, the SAC saw news about a breach at CareFirst and tried to contact Wagner "several times that day."[972] The Special Agent recounted watching the news and deciding to call Wagner. The SAC stated:

> A. It was -- as I recall, it was approximately 6 to 6:30 that night before I was leaving for the day. I called Jeff. Jeff picks up the phone. I was -- almost jumped through the phone, as I recall,

[965] *Id.* at 17-18.
[966] *Id.*
[967] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), available at: https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/.
[968] Council of the Inspectors Gen. on Integrity and Efficiency, *IG Act History*, available at: https://www.ignet.gov/content/ig-act-history (last visited June 4, 2016).
[969] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 3.
[970] Special Agent Tr. at 19.
[971] *Id.*
[972] *Id.* at 19-20.

saying: Jeff, have you heard anything about CareFirst? And Jeff's initial response was: Where are you? And I said: I'm still up in the office. And Jeff said: I need to come see you. So I met him at the door. It was only a few minutes. Jeff was obviously in the building. It was a few minutes. He came up. I escorted him into the conference room. Jeff sat down. And the best way to describe it was, it was totally different than the April meeting that had occurred. I knew something was up just by his body language, and sat down. And Jeff initially said: They got it. I looked at him, and he then repeated: They got all of it. And I asked the question: CareFirst? And he was like, no. I said something to the effect of: How big is this? And as I recall, Jeff said: Homeland Security or US-CERT is down here. FBI is down here. We had a couple of questions, but Jeff just didn't have a lot of information. It was truly different than the April meeting; whereas, you know, we were asking questions, Jeff seemed to be able to respond, this one was certainly not that way.

Q. And did he specifically at this time indicate that background investigation records may have been compromised?

A. He speculated that, yes, they had. But we were -- I was also asking about other systems that are controlled by the Office of Personnel Management, but, yes, Jeff did speculate that background investigations, the SF-86s.[973]

The SAC testified that the scene on May 20, 2015 was dismal, and that it "looked like somebody was defeated. I mean, this was a man who was defeated. The shoulders were slouched, and it had obviously been a -- my recollection, from what I recall, I would classify as a long day."[974]

The SAC accompanied Wagner to meet personnel from the FBI and US-CERT. The Special Agent testified that Wagner said law enforcement personnel were on site, and that Wagner willingly introduced the SAC to the law enforcement officials on site.[975]

Later that day, when the SAC reported the news to OIG colleagues, **nobody was aware of the cyber investigation that was underway just a few floors below**.[976] The SAC stated that after the April 22, 2015 discussion with Wagner, until the May 20, 2015 conversation in the OIG's conference room about the loss of background investigation material, the two had "no substantial conversations."[977] The SAC stated:

---

[973] *Id.* at 20-21.
[974] *Id.* at 45 (emphasis added).
[975] *Id.* at 21.
[976] *Id.* at 22.
[977] *Id.*at 45.

> It was just more work was going on in reference to that. Our conversations primarily focused on, again, the FEHBP carriers and finding out more information about the Anthem breach, finding more information about Premera breach, working with the FBI and what information they needed.[978]

Seymour failed to notify the OIG about the 2014 incident

The IG's notification to Acting Director Cobert did not follow an isolated incident, but rather a series of incidents where it was not notified immediately or promptly by the OCIO. In addition to failing to promptly notify the OIG about the breaches in April 2015 and May 2015, the SAC also testified that the OCIO failed to provide timely notification concerning a breach that US-CERT identified on March 20, 2014 at OPM. The SAC stated:

> Q. Okay. Would you characterize the IG's notification of this March 2014 incident as being timely?
>
> A. No.
>
> Q. Would you characterize it as being in keeping with OPM policy and rules governing notification to the OIG?
>
> A. No.
>
> Q. Today we have discussed three separate cybersecurity incidents occurring at OPM since March 2014. From your perspective, having been involved with all three events, how would you characterize OPM's notification to the Office of Inspector General for these three incidents?
>
> A. I would characterize it as nonexistent. There was -- my opinion -- there was no formal notification to any of these incidents. It was -- the first one, the March 2014, we were notified by another agency; the April 2015, I was just getting off the elevator and happened to be there; and then the May 2015, I proactively reached out to the agency in reference to another issue, and that's how we were notified."[979]

In summary, when McFarland wrote Cobert to raise concerns about the OCIO's failures to notify his office in a timely manner about major cybersecurity events, as the IG Act, FISMA, and OPM's own guidance direct, the IG could have cited even more examples. The OCIO's repeated failure to involve the OIG eroded the relationship between the two offices and prevented the OIG from conducting its important work on behalf of the American public.

---

[978] *Id.* at 43-44.
[979] *Id.* at 26-27.

Meetings with Federal Law Enforcement Agencies

Under OPM's "Incident Response and Reporting Guide," the OIG is "responsible for providing law enforcement authority and investigative support to any incident handling initiatives."[980] The Guide makes clear that the OIG must be notified immediately if criminal activity is suspected, and that "As determined by the OIG, other law enforcement support may be called in to assist in the investigation of an incident."[981]

While the guide clearly states the OIG should be an integral part of any law enforcement activity and determine the need for law enforcement support, the OIG was not even consulted about the need to bring in law enforcement support for this particular incident response. In fact, the OIG was prevented from even attending key meetings with other federal law enforcement agencies. McFarland raised these concerns to Cobert. He wrote:

> During the investigation of the second breach involving background investigation files, the OIG requested to attend meetings between OCIO staff, the Federal Bureau of Investigations (FBI), and the DHS U.S. Computer Emergency Readiness Team (US-CERT). Former Director Archuleta stated that the OIG could not attend these meetings because our presence would 'interfere' with the FBI and US-CERT's work.[982]
>
> * * *
>
> This action is a violation of the Inspector General Act of 1978, as amended (IG Act). The OIG contacted the FBI and US-CERT directly and did indeed meet with them without adversely affecting the progress of the investigation. These meetings provided the OIG with critical information necessary for our own investigatory and audit work. What the former Director considered 'interference' was simply the OIG fulfilling our responsibilities.[983]

The SAC told the Committee that on May 20, 2015, after Wagner relayed that "they got all of it,"[984] the SAC asked Wagner: "Can I go down and meet [law enforcement personnel]?"[985]

The SAC testified: "I immediately asked, because I did not meet the investigators from the previous breach. I wanted to go down, introduce myself, and meet the investigators."[986] Wagner responded, "Absolutely, no problem," and escorted the SAC to a room where "a large number of investigators" were sitting and that "most had been sitting there and had their laptops

---

[980] U.S. Office of Pers. Mgmt., *Incident Response and Reporting Guide* at 3.
[981] *Id.*
[982] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 3.
[983] *Id.* at 3-4.
[984] Special Agent Tr. at 20.
[985] *Id.* at 46.
[986] *Id.*.

up and running."[987] The SAC testified that Wagner introduced him to the law enforcement officials.[988] The SAC offered assistance, and left.[989]

The following day, on May 21, 2015, OPM Director Katherine Archuleta requested a meeting with IG McFarland in the situation room, a small room where classified briefings can occur.[990] McFarland and his Deputy, Norbert ("Bert") Vint, attended the meeting with Archuleta, and they debriefed OIG staff immediately afterwards.[991] The SAC testified that Vint recalled "the Director asked IG McFarland to stop interfering with the investigation."[992] The SAC stated:

> My personal recollection, as I recall, I was stunned at this because the investigator that they were talking about was me. I was there that night receiving the notification from Jeff. I reiterated to both Pat [McFarland] and Bert [Vint] that the May 20th date, I was trying to get ahold of Jeff. There were several times that day I reached out to Jeff; I emailed Jeff; I called Jeff. It was not in reference to this. I had no idea this was going on. Again, I was under the impression that [Wagner] was working the CareFirst breach and [I] wanted more -- desperately wanted more information about this.[993]
>
> * * *
>
> I have never had a situation where the agency has -- I perceived -- as I recall, I perceived it, as the former Director Archuleta was telling Pat [McFarland] that he had a heavy-handed agent who was going down there demanding information. And as I recall, there could be nothing further from the truth. That's why it stands out in my mind. This is such an outlier of anything or any feedback that has ever come from our office. And I recognize there are situations where agencies and IGs may not agree, but to the point where there was a complaint that asserted we were interfering, no, I was just stunned by that.[994]

KeyPoint Audit

Documents and testimony show the OCIO also interfered with the IG's audits. McFarland wrote:

> In October 2014, due to concerns raised after a security breach at United States Investigative Services (USIS) was identified in June 2014, the U.S.

---

[987] *Id.* at 47.
[988] *Id.* at 46-47.
[989] *Id.*.
[990] *Id.* at 23.
[991] *Id.*
[992] *Id.* at 24.
[993] *Id.*
[994] *Id.* at 25.

> Office of Personnel Management (OPM) Office of the Inspector General (OIG) informed the OPM Chief Information Officer (CIO) of our intent to audit KeyPoint Government Solutions (KeyPoint).
>
> At an October 16, 2014 meeting, the CIO requested that we delay this audit, stating that the U.S. Department of Homeland Security (DHS) had just completed a comprehensive assessment of KeyPoint, which was also in response to the USIS breach. Therefore, she was concerned that our audit would interfere with KeyPoint's remediation activity.
>
> The OIG tries to coordinate our oversight work with the OPM program offices to the maximum extent possible, and so we agreed to delay our audit. We later discovered, however, that OPM became aware in early September 2014 that KeyPoint had been breached. Despite knowing this, the CIO did not inform OIG staff of the breach in the October 16th meeting when she requested that we delay our audit work.[995]
>
> * * *
>
> Our audit, which was a comprehensive evaluation of the information technology (IT) security posture of Key Point, was delayed for over three months. The DHS review was focused on incident response objectives, and did not have as wide of a scope as the CIO alluded. In fact, our audit identified a variety of areas that were not part of DHS's review where KeyPoint could improve its IT security controls. The CIO's interference with our audit agenda resulted in additional time passing with these vulnerabilities still present in KeyPoint's environment. The delay also prevented us from communicating important information that may have been relevant to the recent Congressional hearings regarding the OPM data breaches."[996]

This situation is significant and a concern because the OIG has a track record of conducting valuable work related to OPM's security posture. There is no basis—legal or otherwise—for OPM officials to delay or otherwise interfere with the IG's work.

Notification Concerning New IT Infrastructure

The IG alleged the OCIO prevented the IG from being involved in the development of its new IT infrastructure from the start. After a March 2014 cyber incident,[997] OPM/OCIO launched a project to overhaul OPM's IT infrastructure. This project involved a multi-phase approach, including: Tactical (improving the existing security environment), Shell (creating a new data center and IT architecture), Migration (migrating all OPM systems to the new

[995] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 3.
[996] *Id.*
[997] OIG Flash Audit Alert (June 17, 2015) at 5.

architecture), and Cleanup (decommissioning existing hardware and systems).[998] The agency awarded a sole source contract for this multi-phased project, and the contract was initially managed by CIO Seymour.[999]

The IG stated that the OCIO, again, failed to work in good faith with the OIG on this initiative. McFarland wrote:

> The OCIO failed to inform the OIG of a major new initiative to overhaul the agency's IT environment. We did not learn the full scope of the project until March 2015, nearly a year after the agency began planning and implementing the project. This exclusion from a major agency initiative stands in stark contrast to OPM's history of cooperation with our office.[1000]

The IG found out about the IT Infrastructure Improvement project on March 2, 2015, when the Deputy IG met with the OCIO Chief of Staff regarding a special funding request.[1001] Specifically, the IG learned for the first time at this meeting that he was "expected to pay the agency approximately $1.16 million in FY2015 funds" to support the project.[1002] The OCIO Chief of Staff told the Deputy IG that this would be a one-time assessment, but then later was told the assessments would be annual.[1003]

The IT Infrastructure Improvement project implicated a significant amount of money. In late October 2015, OPM advised the Committee that it had spent approximately $60 million in FY2014 and 2015 on the project.[1004] About eighty percent of the funds originated from OPM's revolving fund and the remaining twenty percent from a variety of discretionary and mandatory funds areas.[1005]

According to McFarland, despite the high stakes of the project for IT security, delivery, and costs, the OCIO excluded the OIG. McFarland wrote:

> The role of the OIG is to promote economy, efficiency, and effectiveness in the administration of the agency's programs, as well as to keep the Director, Congress, and the public informed of major problems and deficiencies. Because the OIG was not involved, agency officials were denied the benefit of an independent and objective evaluation of the

---

[998] *Id.*
[999] Imperatis Letter Contract (June 16, 2014), Attach. 1 at 000002 (Imperatis Production: Sept. 1, 2015); *id.* Attach. 1 at 000011. A sole source contract is a contract that was awarded without being subject to the competitive bidding process.
[1000] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 4.
[1001] U.S. Office of Pers. Mgmt., "Background Information: OPM Infrastructure Overhaul and Migration Project" (June 17, 2015) (on file with the Committee).
[1002] *Id.*
[1003] *Id.*
[1004] Email from U.S. Off. of Pers. Mgmt. to H. Comm. on Oversight & Gov't Reform Staff (Oct. 28, 2015) (on file with the Committee).
[1005] *Id.* (OPM requested $21 million in FY2016 to implement and sustain these improvements. The FY2016 omnibus requires OPM to use $21 million of its $272 million appropriated dollars for IT security improvements).

> project's progress from the beginning. The audit work that we have performed since learning of this project has identified serious deficiencies and flaws that would have been much easier to address had we been able to issue recommendations earlier in the project's lifecycle.[1006]

The OCIO's decision to exclude the IG hurt the agency because it lacked information that could have informed the decision-making and planning stages for the IT infrastructure overhaul. The project was exposed to waste, fraud, and abuse partly because of the OCIO's posture with respect to involving the OIG.

Five Incorrect and/or Misleading Statements

McFarland's July 22, 2015 Memorandum cited five incorrect and/or misleading statements to Congress. In the public version of the memorandum, the descriptions of those five incorrect and/or misleading statements were fully redacted.

First Misstatement before the Senate Committee on Appropriations

At a hearing before a Senate Committee on Appropriations' Subcommittee on Financial Servcies and General Government, former Director Katherine Archuleta stated that OPM completed a Major IT Business Case (formerly known as the OMB "Exhibit 300") for the infrastructure improvement project.[1007] McFarland also wrote that "OPM indicated [in response to the flash audit] that they have been in 'continual consultation and discussion with OMB [the Office of Management and Budget]' regarding this project."[1008] According to McFarland, however:

> OPM has not completed a Major IT Business Case, and has not provided us with any evidence that it has consulted with OMB regarding the full scope of the project and that OMB approved OPM's approach. In its June 22nd response to the flash audit alert OPM acknowledged that it has not completed this document (and actually disagrees with our recommendation to prepare one). After the hearing, the OIG again requested documentation supporting OPM's statements, and again the agency has failed to produce any evidence whatsoever that it has kept OMB apprised of the full scope and scale of this project.[1009]

[1006] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 4.
[1007] *OPM Information Technology Spending and Data Security: Hearing Before Subcomm. on Financial Services & Gen. Gov't of the S. Comm. on Appropriations* 114th Cong. at 1:40 (June 23, 2015) [hereinafter *Hearing on OPM Information Technology Spending and Data Security*].
[1008] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 5.
[1009] *Id.*

Second Misstatement Before the Senate Committee on Appropriations

Former Director Archuleta testified at a June 23, 2015 Senate subcommittee hearing that "my CIO has told me that we have, indeed, an inventory of systems and data."[1010] According to McFarland, however:

> Both our flash audit alert and Fiscal Year (FY) 2014 FISMA audit noted that OPM does not maintain a comprehensive inventory of its information technology (IT) assets. We confirmed with the Chief Information Officer (CIO) on June 23, 2015, and again with her staff on June 29th, that OPM is still in the process of developing a comprehensive information system inventory and this process is not yet complete.[1011]

Third Misstatement Before Senate Committee on Appropriations and House Committee on Oversight and Government Reform

Archuleta and Seymour testified before the Senate Appropriations Committee and the House Committee on Oversight and Government Reform that the sole-source contract with Imperatis only covered the first two phases of the IT Infrastructure Improvement project, and that contracts for the migration and cleanup phases of the project had not yet been awarded.[1012] According to McFarland, however:

> The document that justified the sole-source contract clearly stated that it was intended to be used for the full scope of the project, and that full and open competition would be pursued if and when it became appropriate to do so. Further, the statement of work contained in the contract itself specifically states that '[t]he Contractor shall complete the work within this [statement of work] in four different phases: Tactical, Shell, Migration, and Clean Up.' When OIG personnel met with the OCIO on May 26, 2015, to discuss concerns regarding the use of a sole-source contract for all phases of the project, the CIO argued strongly in favor of this approach. She informed us that she wanted the same contractor to oversee all four phases of the project for continuity purposes.[1013]

[1010] *Hearing on OPM Information Technology Spending and Data Security* at 1:40.
[1011] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 5.
[1012] *Hearing on OPM Information Technology Spending and Data Security* at 2:14 (former OPM Director Archuleta: "I would like to remind the Inspector General that contracts for the Migration and Cleanup have not yet been awarded."); *Hearing on OPM Data Breach: Part II* at 2:10.00 (former OPM Director Archuleta: "I would like to remind [the IG] that the contracts for Migration and Cleanup have not yet been awarded. And we will consult with him as we do that."); *id.* at 2:58.00 (CIO Seymour: " ... that's why we only contracted for the first two pieces and we said as we work through this project to understand it, we'll be able to better estimate and understand what needs to move into that Shell.").
[1013] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 6.

Fourth Misstatement Before the House Committee on Oversight and Government Reform

During a hearing before the Committee on Oversight and Government Reform, in response to a question about the eleven systems operating without a valid Security Assessment and Authorization (Authorization) as of the end of FY 2014, Seymour stated this was no longer a concern because she had granted an interim Authorization to these systems.[1014] According to McFarland, however, OMB does not allow interim or extended Authorizations.[1015] Therefore, the CIO's "extension," from the IG's perspective, was not valid, and the eleven systems identified in the 2014 audit have still not been subject to the Authorization process.[1016]

Fifth Misstatement Before the Senate

At a June 25, 2015 Senate hearing, former Director Archuleta stated that OPM had received a special exemption from OMB related to system Authorization because of the ongoing infrastructure improvements.[1017] Office of Management and Budget CIO Tony Scott was unable to confirm this during the hearing.[1018] After the hearing, however, the IG found OMB submitted a request to OPM for evidence supporting this claim. According to McFarland, OPM officials responded by telling OMB that Archuleta did not make such a statement. McFarland found: "This is incorrect, as the statement can be found at timestamp 1:47 of the hearing."[1019]

The agency disagreed with McFarland with respect to the truthfulness of these statements to Congress. The IG's allegations, however, are very serious, and they are supported by documents and other evidence. Providing false testimony to Congress is a crime and these statements should be evaluated by the Department of Justice to determine whether a prosecution may be justified.

Current State of Relationship

McFarland wrote to Cobert: "It is imperative that these concerns be addressed if OPM is to overcome the unprecedented challenges facing it today."[1020] Indeed, OPM has taken actions to improve communication with the OIG. Following the July 2015 memorandum, Cobert

---

[1014] *OPM Data Breach: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. at 2:27.00 (June 16, 2015), available at: https: //oversight.house.gov/hearing/opm-data-breach/ (form OPM CIO Donna K. Seymour: "Sir, I have extended the Authorizations that we had on these systems because we put a number of security controls in place in the environment."). *See also Hearing on OPM Information Technology Spending and Data Security* at 1:36 (former Director Archuleta: "I can tell you that all but one of those systems has been Authorized."); *Hearing on OPM Data Breach: Part II* (statement of former Director Archuleta) ("Of the systems raised in the 2014 audit, 11 of those systems were expired. One of those, a contractor system, is presently expired. All other systems raised in the [2014] audit have either been extended or provided a limited Authorization.").

[1015] OIG Serious Concerns Regarding OCIO (July 22, 2015) at 6.

[1016] *Id.*

[1017] *Id.* at 7.

[1018] *Id.*

[1019] *Id.*

[1020] *Id.* at 1.

instituted regular meetings between the OCIO and OIG to cover key issues, such as planning and new projects.[1021]

> 1) In addition to the bi-weekly meetings we have recently established between you and I (IG-Director Meetings), and the weekly meetings we have recently established between your senior staff and mine (Senior Staff Meetings), we believe we would also both benefit from separate, regularly scheduled meetings between your IT team and OCIO (IG-OCIO Meetings). We propose, at the outset, that we would meet once a month, and can adjust the frequency as needed. We would propose leadership involvement in those meetings, whenever possible, as well. Our OCIO team will come prepared to brief you on recent events and progress on ongoing activities, and you will have the opportunity to raise any questions or concerns on a regular basis. Typical agenda items would include, but not be limited to:
>
> a. Short term and long-term planning;
> b. Proposed new projects;
> c. Updates on ongoing projects, gaps in deliverables, and plans to address any such gaps;
> d. Identification and mitigation of any technical issues that might develop;
> e. FISMA audits and compliance.

OIG Memo, Serious Concerns (July 2015)

In testimony prepared for a February 2016 Committee hearing that was canceled following the resignation of OPM CIO Donna Seymour two days prior, Acting Inspector General Norbert E. Vint stated:

> The productivity of those meetings has improved over time, and through these meetings, we have been able to work through certain issues. The OCIO has also begun to consult with us more often, such as when they instituted the recent '[Authority to Operate] Sprint.'[1022]

Vint stated the relationship improved under Cobert, and that there were no further problems with respect to accessing information.[1023] Vint was prepared to testify that, "Consequently, we have no reason to believe that they have intentionally provided us with inaccurate information or withheld material facts."[1024]

[1021] *Id.*
[1022] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 24, 2016) (prepared statement of Norbert E. Vint, Office of Inspector Gen., U.S. Office of Pers. Mgmt.) (hearing cancelled).
[1023] *Id.*
[1024] *Id.*